Trabajo Fin de Grado

IMPLEMENTACIÓN DEL PROCEDIMIENTO "ATTACH" DE GSM EN PLATAFORMA SOFTWARE DEFINED RADIO

Autor: David Ortega Muñoz

Tutor: Víctor P. Gil Jiménez

Grado en Ingeniería en Tecnologías de Telecomunicación

Universidad Carlos III de Madrid

Escuela Politécnica Superior

Agradecimientos

En primer lugar me gustaría agradecer al Dr. Víctor P. Gil Jiménez por darme la oportunidad de poder adentrarme en el mundo de las comunicaciones móviles y por ayudarme con la realización de este proyecto.

También dar gracias a mi familia por su apoyo y colaboración durante estos cuatro años y a mis amigos y compañeros que hacen los momentos de estudio más fáciles y amenos.

Por último, dar gracias a todos los profesores que me han dado clase durante estos cuatro años por ayudarme a conseguir mi objetivo de ser ingeniero.

Resumen

Este trabajo consiste en realizar una implementación del prodecimiento “attach” de GSM en una plataforma SDR (*Software Defined Radio*). Este procedimiento se produce cuando un móvil se conecta a una red GSM y consiste en un intercambio de mensajes entre la estación base y el móvil en los que se envía información de autenticación para comprobar que el móvil tiene acceso a la red.

Este procedimiento implica a gran parte de la red GSM, pero, este trabajo, únicamente se centra en la interfaz radio. Para ello, se realizaran todos los procesos que llevan a cabo el móvil y la estación base intentando cumplir el estándar GSM lo más fielmente posible.

El trabajo tiene una finalidad docente, con el fin de poder usarse en prácticas de algunas asignaturas relacionadas con los grados de telecomunicaciones.

Palabras clave: SDR, LabVIEW, USRP, GSM, attach.

Abstract

This degree thesis is the attach procedure of GSM in a SDR (*Software Defined Radio*) platform. This procedure takes place when a mobile is connected to a GSM network and it consists in an exchange of messages between the base station and the mobile in which authentication information is sent to verify that the mobile has access network.

This procedure involves a big part of the GSM network, but this project is only focused on the radio interface. In order to do this, all the processes that the mobile and the base station perform will be conducted, trying to meet the GSM standards as accurately as possible.

The purpose of this work has an academic nature, because this implementation can be used in different practices of related telecommunication subjects.

Keywords: SDR, LabVIEW, USRP, GSM, attach.

Contenido

Índice de Figuras

Índice de tablas

Índice de ecuaciones

Glosario

ADC	*Analog to Digital Converter*	Conversor analógico digital
AGCH	*Access Grant CHannel*	Canal de concesión de acceso
AuC	*Authentication Center*	Centro de Autenticación
BCCH	*Broadcast Control CHannel*	Canal de control de difusión
BSC	*Base Station Controller*	Controlador de estación base
BSIC	*Base Station Identity Code*	Código de Identidad de la Estación Base
BSS	*Base Station Subsystem*	Subsistema de estación base
BTS	*Base Transceiver Station*	Transceptor de estación base
CBCH	*Cell Broadcast Channel.*	Canal de difusión de celda
CCCH	*Common Control CHannel*	Canal de Control Común
CCH	*Control CHannel*	Canal de control
EIR	*Equipment Identity Register*	Registro de identidades de equipos
FCCH:	*Frequency Control CHannel*	Canal de Control de Frecuencia
FDD	*Frequency Division Duplexing*	Duplexación por División en la Frecuencia

FDMA	*Frequency Division Multiple Access*	Acceso Múltiple por División en la Frecuencia
GMSK	*Gaussian Minimum Shift Keying*	Modulación por desplazamiento mínimo con pulsos *gaussianos*
GPRS	*Global Packet Radio Service*	Servicio General de Paquetes vía Radio
GSM	*Global System for Mobile*	Sistema Global para las comunicaciones Móviles
HLR	*Home Location Register*	Registro local de abonados
IMSI	*International Mobile Subscriber Identity*	Identidad internacional del abonado móvil
ISDN	*Integrated Services Digital Network*	Red digital de servicios integrados
LabVIEW	*Laboratory Virtual Instrumentation Engineering Workbench*	
ME	*Mobile Equipment*	Equipo móvil
MS	*Mobile Station*	Estación Móvil.
MSC	*Mobile Switching Center*	Centro de conmutación móvil
MSISDN	*Mobile Subscriber ISDN Number*	Número de abonado móvil para ISDN
MSRN	*Mobile Subscriber Roaming Number*	Numero de abonado móvil para itinerancia
NCH	*Notification CHannel*	Canal de notificaciones
NI	*National Instruments*	
NMC	*Network Management Center*	Centro de gestión de red

NMT	*Nordic Mobile Telephony*	Telefonía móvil nórdica
NSS	*Network and Switching Subsystem*	Subsistema de red y conmutación
OMC	*Operation and Maintenance Center*	Centro de mantenimiento y operación
OMSS	*Operation and Maintenance SubSystem*	Subsistema de operación y mantenimiento
PC	*Personal Computer*	Ordenador Personal
PCH	*Paging CHannel*	Canal de localización
PDN	*Public Data Network*	Red pública de datos
PLMN	*Public Land Mobile Network*	Red móvil pública terrestre
PSTN	*Public Switched Telephone Network*	Red telefónica pública conmutada
RACH	*Random Access CHannel*	Canal de Acceso Aleatorio
RF	*Radio Frequency*	Radio Frecuencia
RPE-LTP	*Regular Pulse Excitation – Long Term Prediction*	Predicción a largo plazo por excitación del pulso regular
SAR	*Specific Absorption Rate*	Tasa de absorción específica
SCH	*Synchronization CHannel*	Canal de sincronización
SDCCH	*Stand-alone Dedicated Control CHannel*	Canal de control dedicado
SDR	*Software Defined Radio*	Radio definido por software

SIM	*Subscriber Identity Module*	Módulo de Identidad del abonado
SMS	*Short Message Service*	Servicio de mensajes cortos
TCH	*Traffic CHannel*	Canal de tráfico
TDMA	*Time Division Multiple Access*	Acceso múltiple por división en el tiempo
TFG		Trabajo Fin de Grado
TIC		Tecnologías de la Información y la Comunicación
TMSI	*Temporary Mobile Subscriber Identity*	Identidad temporal del abonado móvil
TN	*Time Slot Number*	Número de intervalo de tiempo (*time slot*)
TS	*Training Sequence*	Secuencia de entrenamiento
TSC	*Training Sequence Code*	Código de la secuencia de entrenamiento
UMTS	*Universal Mobile Telecommunications System*	Sistema de Telecomunicaciones Móviles Universal
USRP	*Universal Software Radio Peripheral*	Software universal para radio periférico
VI	*Virtual Instrument*	Instrumento Virtual
VLR	*Visitor Location Register*	Registro de Localización de Visitantes

1. Selected sections in English

1.1 Introduction

1.1.1 Objetives

The main goal of this project is to perform an implementation of the attach procedure in GSM on a Software Defined Radio platform using USRP transceivers. The purpose of this work has an academic nature, because this implementation can be used in different practices of subjects as telecommunication systems or mobile communications in academic degrees related to telecommunications.

The entire system will have an implementation of the GSM base station and another implementation of the mobile station to communicate between them by sending messages needed to perform the attach procedure.

In this work only the radio interface is implemented, allowing for possible extensions the communication with other network elements.

Due to the didactic purpose of this project, the implementation must be configurable and easy to use, not only for its practical application, but to being able to enhance the functionality and to use parts of this work for future projects.

In the beginning, the system could be formed by two unique USRP, but, to avoid possible limitations of the transceivers, the implementation will be carried out with four USRP transceivers, two of them will make up the GSM base station and two will make up the mobile station. These transceivers will be controlled by a computer using LabVIEW.

In addition, this project will use some modules used in previous works related to GSM, so this project could be considered an extension of previous projects.

1.1.2 Memory organization

This report was written after making the most of the practical work required. In addition, this practical work was developed following a process of in-depth theoretical study of all the parts involved in this work, such as GSM standards or all necessary working environment (both hardware and software).

The memory will consist of two parts. The first part will be composed by the theoretical analysis of the project, describing the most important things needed to

understand the project, while the second part will be focused on the practical part developed to meet the required functionalities.

The theoretical part of the project will be composed by an introduction, problem statement, where details as state of art or regulatory framework will be detailed, GSM standard characteristics and a description of the work environment.

In the practical part, there will be a detailed description of the design and development work, highlighting the most important parts and a sample of the results obtained from the tests.

Finally, there will be a detailed budget and the final conclusions.

The chapters of this work are:

- Chapter 1: Introduction: Describes the work objectives and motivations, memory structure and timetable.
- Chapter 2: Problem statement: Includes related aspects with the project as state of art and regulatory framework.
- Chapter 3: GSM standard: Describes some GMS aspects related to the project.
- Chapter 4: Work environment: Describes all the hardware and software used to perform the work.
- Chapter 5: Design and development: Shows all the performed work.
- Chapter 6: Test and results: Presents conducted test and the obtained results.
- Chapter 7: Budget: Detailed budget of the work. It includes cost of staff and materials.
- Chapter 8: Conclusions: Presents the conclusions that have been reached after the job.

1.1.3 Timetable.

This project began in February and finished in mid-September, so it lasted 7 months approximately. This calendar does not contain weekends and the next holidays:

- March 17: San José day.
- From March 30 to April 6: Holy Week.
- May 1: International Workers' Day.
- June 4: Corpus Christi.
- August 17: Local holiday in Leganés.

The development of this work has followed structured and defined stages as follows:

1. Documentation about GSM.
   1.1. Search and selection of GSM documentation: 3 days

1.2. In-depth study of documents: 15 days

2. Learning and familiarization with tools.
   2.1. Learning LabVIEW graphical language: 15 days
   2.2. Getting know the used hardware (NI-USRP and vector signal analyzer): 5 days
3. Implementation of the modules.
   3.1. Testing and verification of the modules already completed: 5 days
   3.2. Implementation of needed modules: 60 days
4. Test and optimization: 15 days
5. Making of the memory: 30 days

1.1.3.1 Phase 1

This first phase was conducted between February 2 and February 25. In this first phase it was collected and selected all documentation on GSM necessary to do the job. Also, documentation was study in-depth and Matlab examples were done.

1.1.3.2 Phase 2

In the phase 2, the work is focused on becoming familiar with work tools. The first part of this phase is dedicated to learn LabVIEW software. For that, some tutorials and test were done. The second part is to becoming familiar with hardware, making some test with transceivers and using little programs made with LabVIEW.

1.1.3.3 Phase 3

This phase is the most important of the project because in it all the main work was done. The first days were used to check all previous modules done by another partners. The rest of the time was used to make all necessary modules to carry out all work.

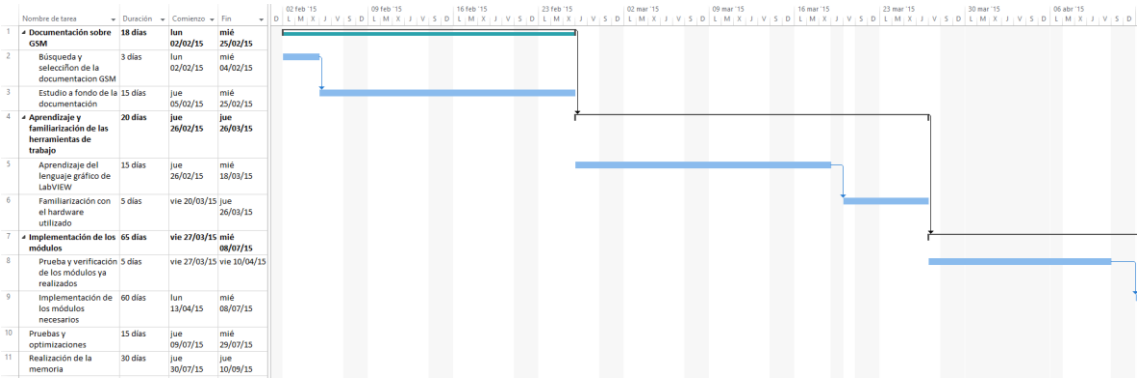
1.1.3.4 Phase 4

The phase 4 was dedicated to testing all modules and the whole work. This testing phase was performed after making modules but was also performed during programming.

1.1.3.5 Phase 5

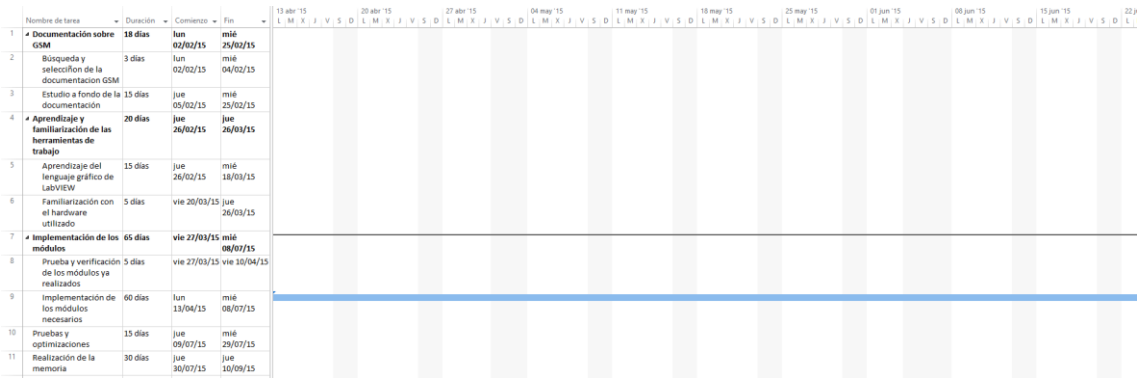
The last phase was dedicated to write the memory.

The next images show the Gantt Diagram of the Project:



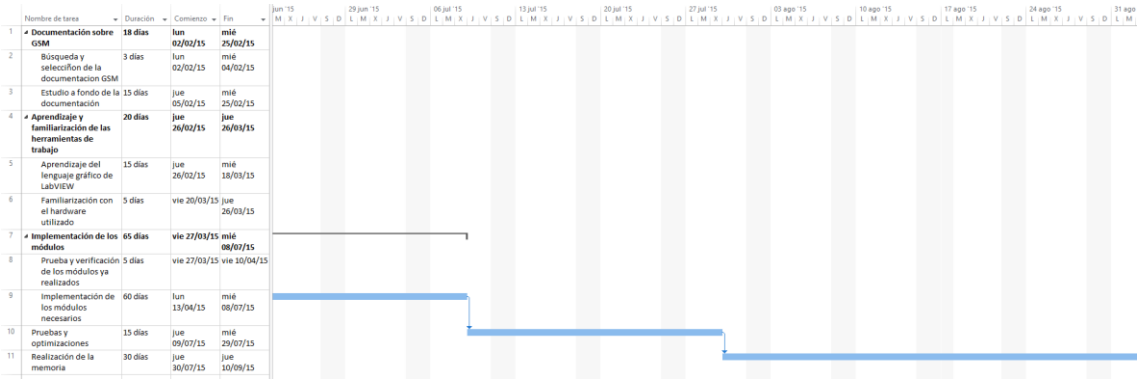
	Nombre de tarea	Duración	Comienzo	Fin
1	**Documentación sobre GSM**	**18 días**	**lun 02/02/15**	**mié 25/02/15**
2	Búsqueda y selecciñon de la documentacion GSM	3 días	lun 02/02/15	mié 04/02/15
3	Estudio a fondo de la documentación	15 días	jue 05/02/15	mié 25/02/15
4	**Aprendizaje y familiarización de las herramientas de trabajo**	**20 días**	**jue 26/02/15**	**jue 26/03/15**
5	Aprendizaje del lenguaje gráfico de LabVIEW	15 días	jue 26/02/15	mié 18/03/15
6	Familiarización con el hardware utilizado	5 días	vie 20/03/15	jue 26/03/15
7	**Implementación de los módulos**	**65 días**	**vie 27/03/15**	**mié 08/07/15**
8	Prueba y verificación de los módulos ya realizados	5 días	vie 27/03/15	vie 10/04/15
9	Implementación de los módulos necesarios	60 días	lun 13/04/15	mié 08/07/15
10	Pruebas y optimizaciones	15 días	jue 09/07/15	mié 29/07/15
11	Realización de la memoria	30 días	jue 30/07/15	jue 10/09/15

Figure 1: Gantt Diagram (part 1)



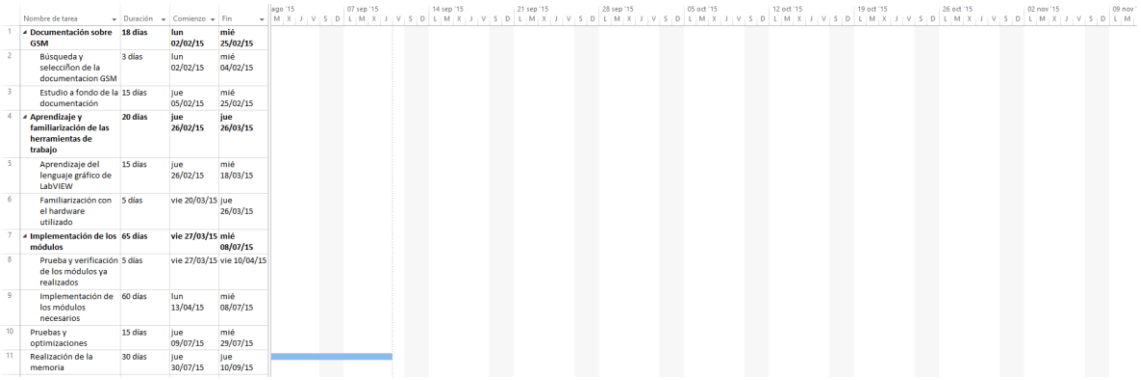
	Nombre de tarea	Duración	Comienzo	Fin
1	**Documentación sobre GSM**	**18 días**	**lun 02/02/15**	**mié 25/02/15**
2	Búsqueda y selecciñon de la documentacion GSM	3 días	lun 02/02/15	mié 04/02/15
3	Estudio a fondo de la documentación	15 días	jue 05/02/15	mié 25/02/15
4	**Aprendizaje y familiarización de las herramientas de trabajo**	**20 días**	**jue 26/02/15**	**jue 26/03/15**
5	Aprendizaje del lenguaje gráfico de LabVIEW	15 días	jue 26/02/15	mié 18/03/15
6	Familiarización con el hardware utilizado	5 días	vie 20/03/15	jue 26/03/15
7	**Implementación de los módulos**	**65 días**	**vie 27/03/15**	**mié 08/07/15**
8	Prueba y verificación de los módulos ya realizados	5 días	vie 27/03/15	vie 10/04/15
9	Implementación de los módulos necesarios	60 días	lun 13/04/15	mié 08/07/15
10	Pruebas y optimizaciones	15 días	jue 09/07/15	mié 29/07/15
11	Realización de la memoria	30 días	jue 30/07/15	jue 10/09/15

Figure 2: Gantt Diagram (part 2)



	Nombre de tarea	Duración	Comienzo	Fin
1	**Documentación sobre GSM**	**18 días**	**lun 02/02/15**	**mié 25/02/15**
2	Búsqueda y selecciñon de la documentacion GSM	3 días	lun 02/02/15	mié 04/02/15
3	Estudio a fondo de la documentación	15 días	jue 05/02/15	mié 25/02/15
4	**Aprendizaje y familiarización de las herramientas de trabajo**	**20 días**	**jue 26/02/15**	**jue 26/03/15**
5	Aprendizaje del lenguaje gráfico de LabVIEW	15 días	jue 26/02/15	mié 18/03/15
6	Familiarización con el hardware utilizado	5 días	vie 20/03/15	jue 26/03/15
7	**Implementación de los módulos**	**65 días**	**vie 27/03/15**	**mié 08/07/15**
8	Prueba y verificación de los módulos ya realizados	5 días	vie 27/03/15	vie 10/04/15
9	Implementación de los módulos necesarios	60 días	lun 13/04/15	mié 08/07/15
10	Pruebas y optimizaciones	15 días	jue 09/07/15	mié 29/07/15
11	Realización de la memoria	30 días	jue 30/07/15	jue 10/09/15

Figure 3: Gantt Diagram (part 3)



	Nombre de tarea	Duración	Comienzo	Fin
1	**Documentación sobre GSM**	**18 días**	**lun 02/02/15**	**mié 25/02/15**
2	Búsqueda y selecciñon de la documentacion GSM	3 días	lun 02/02/15	mié 04/02/15
3	Estudio a fondo de la documentación	15 días	jue 05/02/15	mié 25/02/15
4	**Aprendizaje y familiarización de las herramientas de trabajo**	**20 días**	**jue 26/02/15**	**jue 26/03/15**
5	Aprendizaje del lenguaje gráfico de LabVIEW	15 días	jue 26/02/15	mié 18/03/15
6	Familiarización con el hardware utilizado	5 días	vie 20/03/15	jue 26/03/15
7	**Implementación de los módulos**	**65 días**	**vie 27/03/15**	**mié 08/07/15**
8	Prueba y verificación de los módulos ya realizados	5 días	vie 27/03/15	vie 10/04/15
9	Implementación de los módulos necesarios	60 días	lun 13/04/15	mié 08/07/15
10	Pruebas y optimizaciones	15 días	jue 09/07/15	mié 29/07/15
11	Realización de la memoria	30 días	jue 30/07/15	jue 10/09/15

Figure 4: Gantt Diagram (part 4)

As shown in the Gantt diagram, critical path pass through all the tasks, because to begin the next phase of the work the previous one must be done.

1.2 Extended abstract

This section presents a summary of the more important items of the job.

The main topic of this dissertation is mobile communication, especially GSM. GSM started as a project for a global mobile communications system. The standard was first developed in 1982 and in 1990 GSM-900 specifications were presented.

This project tries to perform a simulation of the attach procedure in GSM. To do that a Software Defined Radio platform was used. A Software Defined Radio platform is usually composed by a radio frequency adapter, an analogic-digital converter and a computer that is responsible for all signal processing and all the necessary operations.

In this case, LabVIEW and four NI-USRP 2920 transceivers were used. LabVIEW by National instrument is a graphical programming environment. The NI-USRP transceivers are used to send and receive signals. To control this transceivers, two computers where used. Furthermore, an Agilent VSA (*Vector Signal Analyzer*) 89600S is used for testing.

The attach procedure is executed when a Mobile Station is switched ON. In this procedure, the Mobile Station has to authenticate in the network. Attach procedure has the following steps [1]:

1. The MS will send a Channel Request message to the BSS on the RACH.
2. The BSS responds on the AGCH with an Immediate Assignment message and assigns an SDCCH to the MS.
3. The MS immediately switches to the assigned SDCCH and sends a Location Update Request to the BSS. The MS will send either an IMSI or a TMSI to the BSS.
4. The BSS will acknowledge the message. This acknowledgement only tells the MS that the BTS has received the message, it does not indicate the location update has been processed.
5. The BSS forwards the Location Update Request to the MSC/VLR.
6. The MSC/VLR forwards the IMSI to the HLR and requests verification of the IMSI as well as Authentication Triplets.

7. The HLR will forward the IMSI to the Authentication Center (AuC) and request authentication triplets.
8. The AuC generates the triplets and sends them along with the IMSI, back to the HLR.
9. The HLR validates the IMSI by ensuring it is allowed on the network and is allowed subscriber services. It then forwards the IMSI and Triplets to the MSC/VLR.
10. The MSC/VLR stores the SRES and the Kc and forwards the RAND to the BSS and orders the BSS to authenticate the MS.
11. The BSS sends the MS an Authentication Request message. The only parameter sent in the message is the RAND.
12. The MS uses the RAND to calculate the SRES and sends the SRES back to the BSS on the SDCCH in an Authentication Response. The BSS forwards the SRES up to the MSC/VLR.
13. The MSC/VLR compares the SRES generated by the AuC with the SRES generated by the MS. If they match, then authentication is completed successfully.
14. The MSC/VLR forwards the Kc for the MS to the BSS. The Kc is NOT sent across the Air Interface to the MS. The BSS stores the Kc and forwards the Set Cipher Mode command to the MS. The CIPH_MOD_CMD only tells the MS which encryption to use (A5/X), no other information is included.
15. The MS immediately switches to cipher mode using the A5 encryption algorithm. All transmissions are now enciphered. It sends a Ciphering Mode Complete message to the BSS.
16. The MSC/VLR sends a Location Updating Accept message to the BSS. It also generates a new TMSI for the MS. TMSI assignment is a function of the VLR. The BSS will either send the TMSI in the LOC_UPD_ACC message or it will send a separate TMSI Reallocation Command message. In both cases, since the Air Interface is now in cipher mode, the TMSI is not compromised.
17. The MS sends a TMSI Reallocation Complete message up to the MSC/VLR.
18. The BSS instructs the MS to go into idle mode by sending it a Channel Release message. The BSS then deassigns the SDCCH.

19. The MSC/VLR sends an Update Location message to the HLR. The HLR records which MSC/VLR the MS is currently in, so it knows which MSC to point to when it is queried for the location of the MS.

This project only simulate the radio interface between Mobile Station and Base Station so, message exchange is:

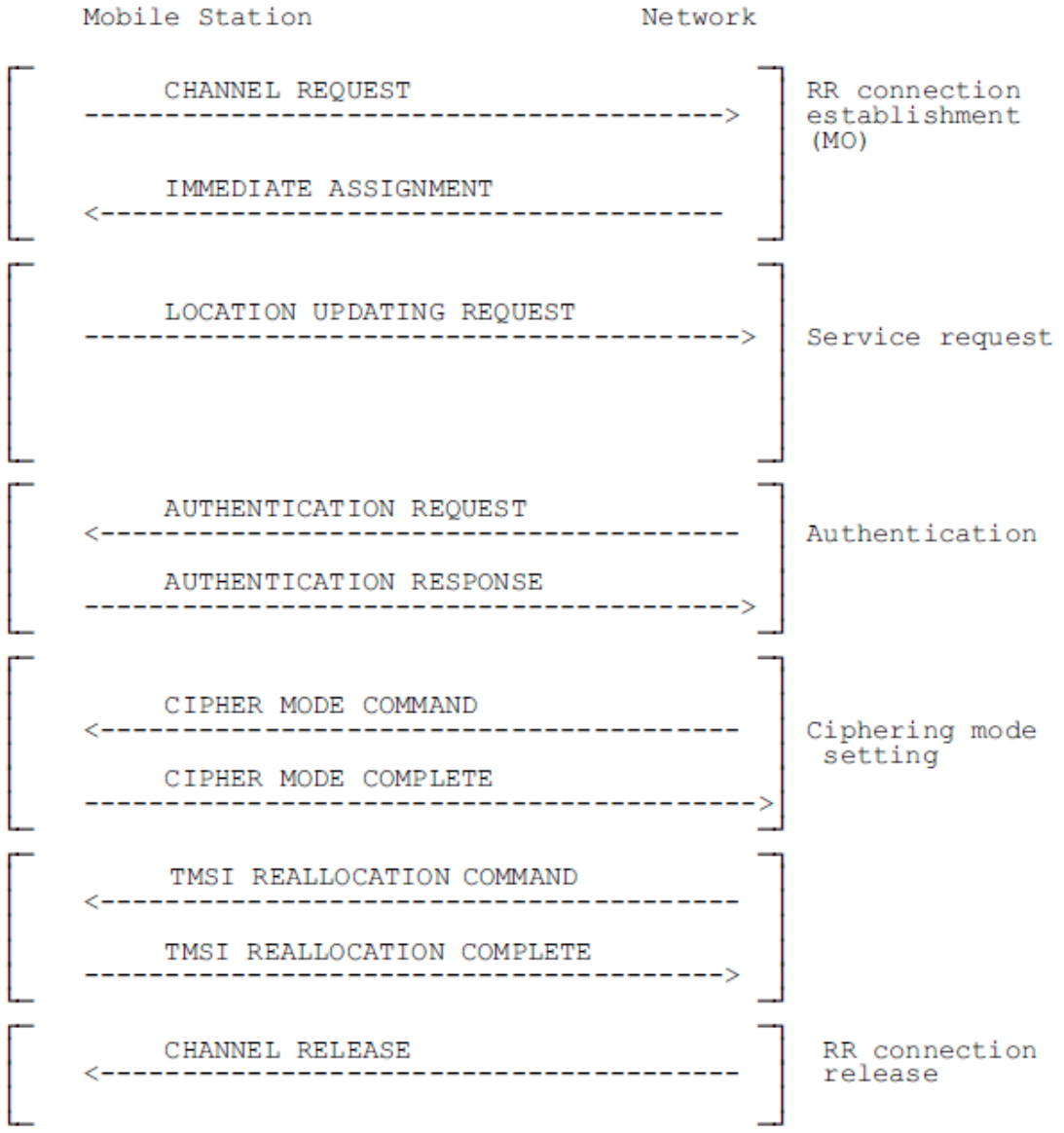


Figure 5: Messages exchange [2]

To achieve this goal is needed performing a series of modules and functions:

- Perform an implementation of the RACH, AGCH and SDCCH channels with their respective coding and decoding.
- Develop modules that have output messages needed to perform the procedure.

- Develop modules for transmission and reception of these messages including the GMSK modulation used in GSM.
- Perform a user interface to interact with the program.

1.2.1 RACH Channel

RACH is a common control channel used for unscheduled requests, in this case, a channel request to do attach procedure.

On the RACH channel 8 bits of useful information that are coded as follows are transmitting:

1. Six parity bits.
2. Four tail bits.
3. Convolutional encoder ½.

The module where the encoding is performed is RACH.vi

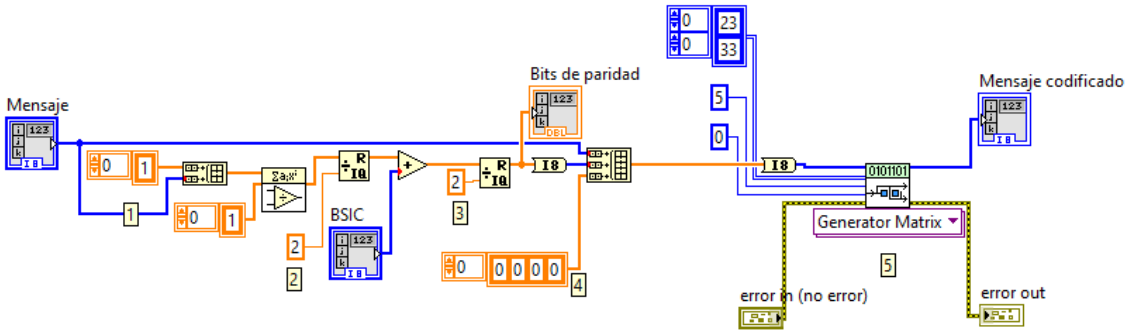


Figure 6: RACH encoding

The decoding is composed only by convolucional decoder and parity and tail bits are eliminated. This module is Decodificador RACH.vi

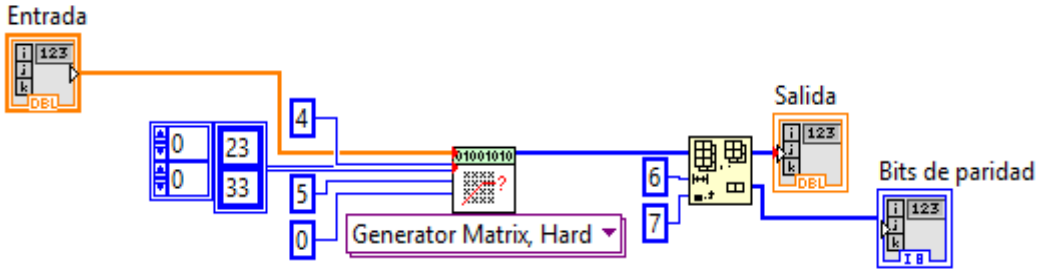


Figure 7: RACH decoding

1.2.2 SDCCH and AGCH Channels

On the SDCCH and AGCH channels 184 bits of useful information that are coded as follows are transmitting:

1. Block code.
   1.1. Forty parity bits based on a FIRE code.
   1.2. Four tail bits.
2. Convolutional encoder ½.
3. Interleaving.

Three modules are involved in this channels.

The interleaving is done in entrelazado.vi:

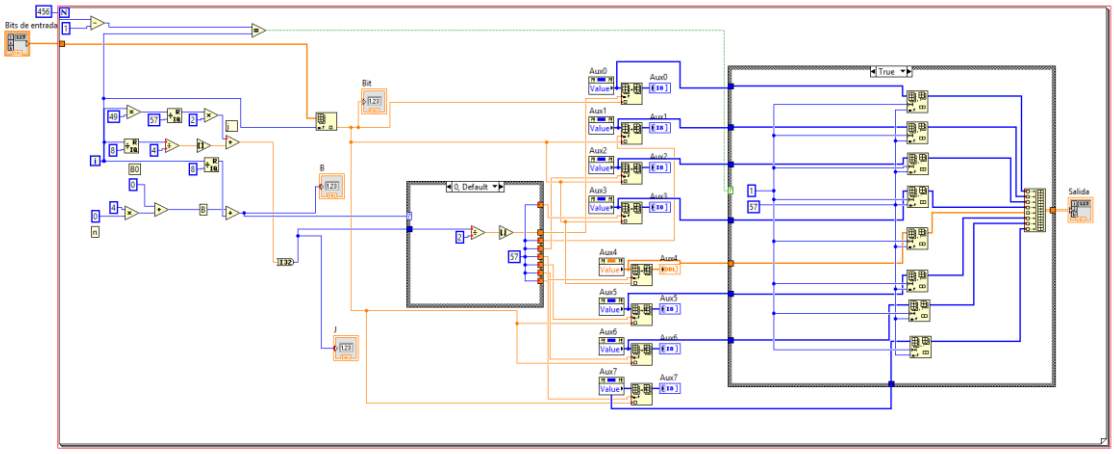


Figure 8: Interleaving

The channel encoding is done in SDCCH.vi where entrelazado.vi is used:

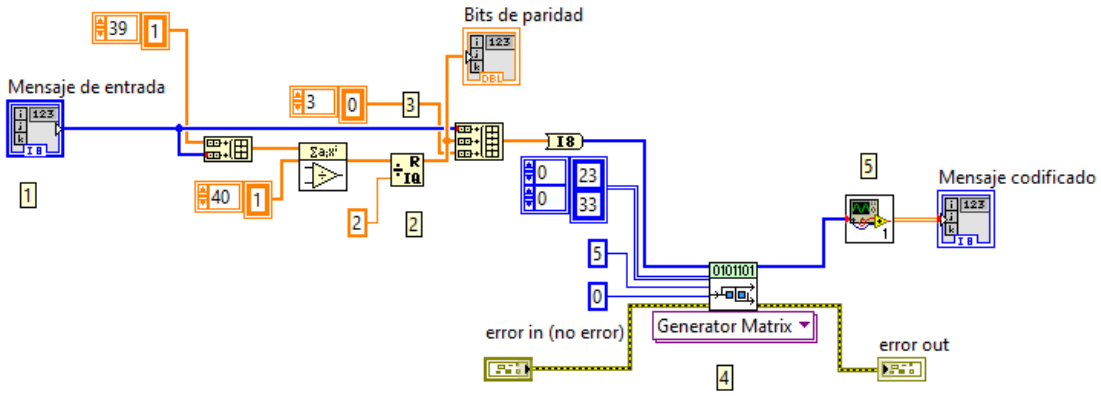


Figure 9: SDCCH encoding

Finally, channel decoding is done in Decodificador SDCCH.vi where interleaving and convolucional decoding are involved:

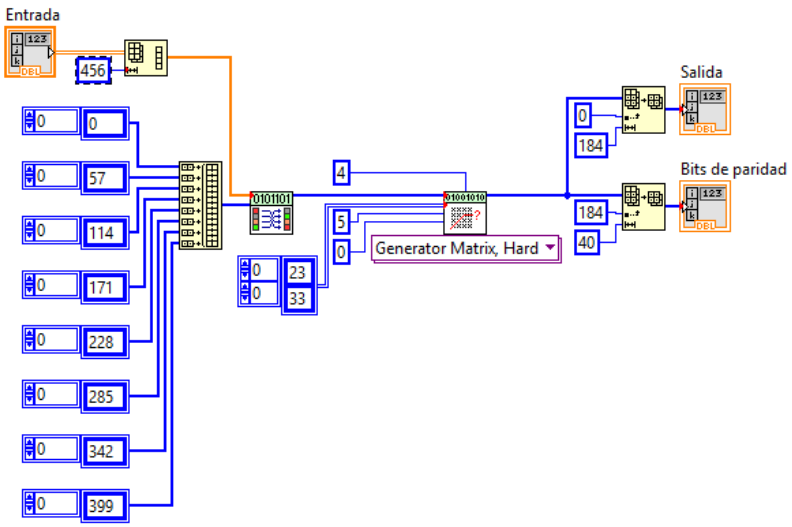


Figure 10: SDCCH decoding

1.2.3 Messages

Every message used in this project has his vi. In these vi, the message is formed by all fields that composed each message.

1.2.4 Insertion in the burst

Once we have all the messages and the encoding, the result has to be inserted in a burst. The RACH channel uses an Access Burst and SDCCH and AGCH use a Normal Burst.

1.2.4.1 Access Burst

Access Burst is used to random network access. It is composed by:

TB 3	41 Bits SYN	36 Bits datos cifrados	TB 3	GP 68,25

Figure 11: Access burst [3]

1.2.4.2 Normal Burst

Normal burst is the most used burst in GSM. It is used by traffic channels and most of control channels. It is composed by:

TB 3	58 Bits datos cifrados	26 Bits TS	58 Bits datos cifrados	TB 3	GP 8,25

Figure 12: Normal burst [3]

1.2.5 Modulation

When burst are done, 8 burst are gathered to get a frame. This frame is modulate according to GSM standard in Modulador.vi:

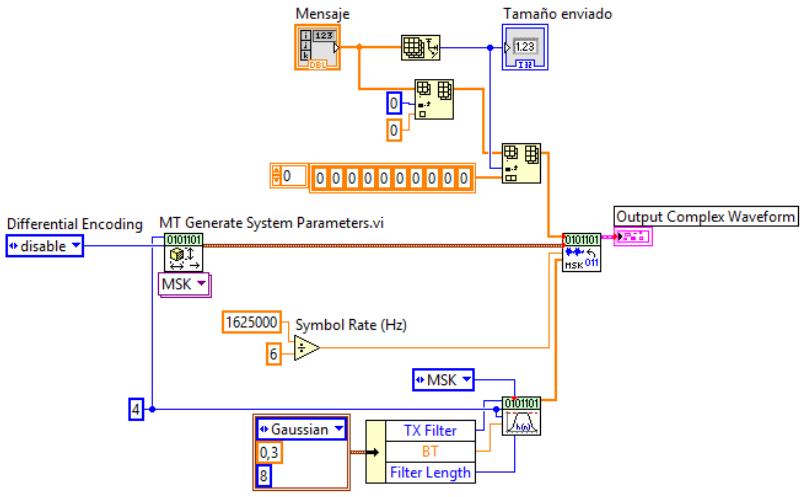


Figure 13: Modulation

The modulation parameters are:

- Modulation type: MSK.
- Samples per symbol: 4.
- Filter type: Gaussian.
- BT: 0.3.
- Filter length: 8 symbols.
- Symbol rate: 270833.33 Hz.

1.2.6 Demodulation

Demodulation has a similar LabVIEW code to modulation. The parameters are the same.

1.2.7 User Interface

Gathered all these modules and some more, the entire system is complete. To make easy to use, the program has two user interface one for Mobile Station and one for BTS. Both interfaces has next parameters and indicators:

- Configuration parameters for USRP.
- BSIC and Buffer size.
- Transmitter and receiver state.
- Attach procedure state.

- Received and decoded message.

The interfaces look as follows:

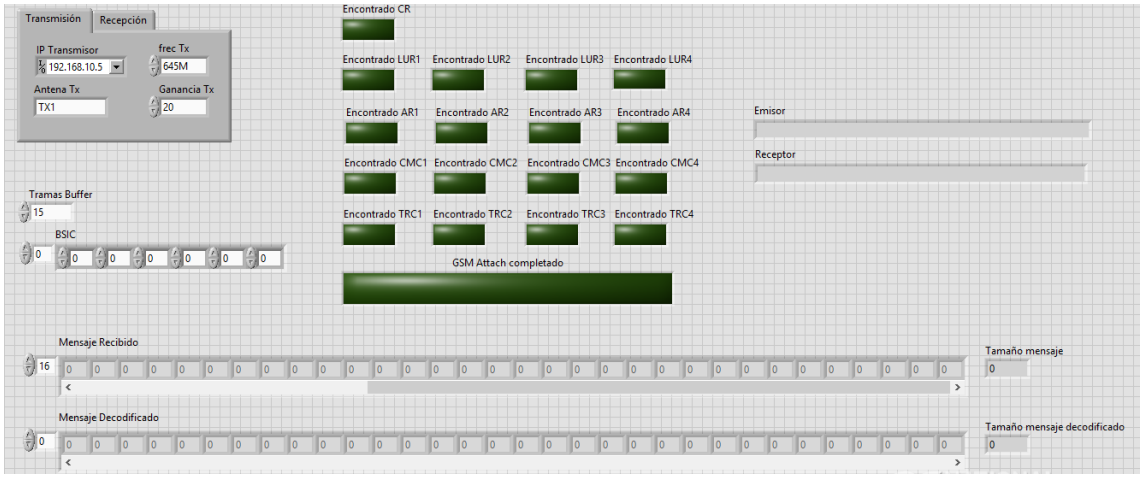


Figura 14: BTS user interface

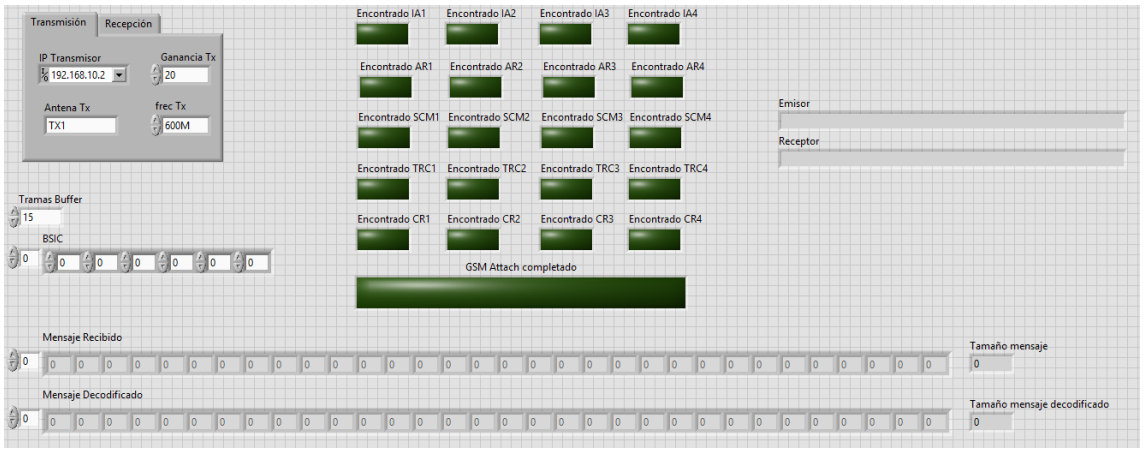


Figure 15: Mobile Station user interface

1.2.8 Test and results

During development of the program, some test were made, majority, in encoding and decoding.

The most important test were done when programming finished. For these test, vector signal analyzer was used. Some of these test are:

- Spectrum.
- Correct operation of the channels (RACH, AGCH and SDCCH).
- Received constellation.

1.3 Conclusions

1.3.1 General conclusions

The results shown in chapters 4 and 5 show that, broadly speaking, the goal of this work has been achieved. Despite some complications, it has achieved the necessary exchange of messages between the base station and mobile to perform the attach procedure described.

Regarding the goal of implementing the procedure as closely as possible to the standard, it hasn't been fully achieved.

The creation of messages, insertion in the burst, coding, and, finally, its modulation is achieved as indicated by the GSM standard. However, the sending and receiving of messages has been giving many problems, so part of the radio interface does not really fit to GSM. In this case, synchronization has not been possible, so the receiver has to detect patterns in order to get messages sent to it by the other part.

Despite these problems, the academic purpose of this project is achieved. The work shows many processes performed in GSM and can be used to bring this technology to other students. In addition, this work would be used in future projects.

Following the completion of this work, the student has managed to check the advantages and disadvantages of using SDR technologies. On the one hand, the student has perceived the great potential of these technologies, which, using a laptop and receivers and transmitters can get results that can be used in the real world. However, on the other hand, it has seen the complexity of software that may have these systems, because, although the costs are much cheaper because of the hardware, the software behind it can become very complex.

1.3.2 Further work

This work can have future lines of work such as:

- Work can be complete by performing synchronization between base station and mobile station.
- The attach procedure is not unique of GSM, so this procedure can be implemented in another technologies as GRPS, UMTS or LTE.
- This work is focused on radio interface. In future works, the student can add another network elements as MSC or HLR.

As shown, there may be several lines of future work, although they may be limited by the capacity of the transceivers available.

2. Introducción

2.1 Objetivos

El objetivo principal de este proyecto es realizar una implementación del procedimiento de attach en GSM en una plataforma Software Defined Radio utilizando transceptores USRP. La finalidad de este proyecto es de carácter docente, ya que esta implementación podrá ser utilizada en distintas prácticas de asignaturas como sistemas de telecomunicación o comunicaciones móviles en los grados relacionados con las telecomunicaciones.

El sistema completo contará con una implementación de la estación base GSM y otra implementación de una estación móvil que se comunicarán entre ellas enviando los mensajes necesarios para realizar el procedimiento de attach.

En este trabajo únicamente se implementará la interfaz radio entre la BTS y la estación móvil, dejando para posibles ampliaciones la comunicación con los demás elementos de la red.

Debido a la finalidad didáctica de este proyecto, la implementación deberá ser configurable y sencilla de usar, no solo para el uso en las prácticas, sino para poder realizar ampliaciones e ir añadiendo módulos para mejorar las funcionalidades y para poder usar partes de este trabajo en futuros proyectos.

El sistema, en principio, podría estar formado por dos únicos USRP, pero para evitar posibles limitaciones de los transceptores, la implementación se realizará con cuatro transceptores USRP, dos de ellos formaran la estación base de GSM y los otros dos el terminal móvil. Estos transceptores estarán controlados por un ordenador usando el entorno de trabajo LabVIEW.

Además, el trabajo usará módulos previamente realizados en otros trabajos fin de grado en los que se han realizado otras implementaciones relacionadas con GSM, por lo que se podría considerar una ampliación de trabajos anteriores.

2.2 Organización de la memoria

Esta memoria se escribió tras realizar la mayor parte del trabajo práctico requerido. Además, dicho trabajo se desarrolló tras un proceso de estudio teórico en profundidad de todas las partes involucradas en este trabajo, como la documentación de GSM o todo el entorno de trabajo necesario para realizarlo (tanto hardware como software).

La memoria estará compuesta por dos grandes partes. Una primera parte estará formada por el análisis teórico del proyecto, describiendo las partes más importantes necesarias para entender el proyecto, mientras que la segunda parte se centrará en la parte práctica desarrollada para cumplir las funcionalidades requeridas.

La parte teórica del proyecto estará formada por una introducción, el planteamiento del problema en el que se detallaran detalles como el estado del arte o el marco regulador en el que encaja el proyecto, características del estándar GSM y la descripción del entorno de trabajo utilizado.

En cuanto a la parte práctica, se hará una descripción detallada del diseño y desarrollo del trabajo, destacando las partes más importantes del mismo y una muestra de los resultados obtenidos mediante las pruebas.

Por último, se presentará un presupuesto detallado del trabajo y las conclusiones a las que se han llegado tras realizarlo.

Los capítulos que componen este trabajo son los siguientes:

- **Capítulo 1:** Introducción: Describe los objetivos y motivación del trabajo, la estructura de la memoria y el cronograma seguido para realizarlo.
- **Capítulo 2:** Planteamiento del problema: Incluye aspectos relacionados con el trabajo como el estado del arte y el marco regulador.
- **Capítulo 3:** Estándar GSM: Describe ciertos aspectos de GSM relacionados con el trabajo a realizar.
- **Capítulo 4:** Entorno de trabajo: Describe todo el hardware y software utilizado para realizar el trabajo.
- **Capítulo 5:** Diseño y desarrollo: Describe todo el trabajo práctico realizado.
- **Capítulo 6:** Pruebas y resultados: Presenta las pruebas realizadas al trabajo y los resultados obtenidos en ellas.
- **Capítulo 7:** Presupuesto: Presupuesto detallado del trabajo. Incluye costes de personal y de material.
- **Capítulo 8:** Conclusiones: Presenta las conclusiones a las que se han llegado tras realizar el trabajo.

2.3 Cronograma

Este proyecto comenzó el mes de febrero y finalizó a mediados de septiembre, es decir tuvo una duración de, aproximadamente, 7 meses y medio. Este calendario no incluye fines de semana ni los siguientes días festivos:

- 17 de marzo: Día de San José.
- Del 30 de marzo al 6 de abril: Semana Santa.
- 1 de mayo: Día Internacional de los Trabajadores.
- 4 junio: Corpus Christi.
- 17 de agosto: Fiesta local de Leganés.

El desarrollo de este trabajo ha seguido unas fases definidas y estructuradas de la siguiente forma:

1. Documentación sobre GSM.
   1.1. Búsqueda y selección de la documentación de GSM: 3 días
   1.2. Estudio a fondo de la documentación: 15 días
2. Aprendizaje y familiarización de las herramientas de trabajo.
   2.1. Aprendizaje del lenguaje gráfico de LabVIEW: 15 días
   2.2. Familiarización con el hardware utilizado (NI-USRP y analizador vectorial de señales): 5 días
3. Implementación de los módulos.
   3.1. Prueba y verificación de los módulos ya realizados: 5 días
   3.2. Implementación de los módulos necesarios: 60 días
4. Pruebas y optimizaciones: 15 días
5. Realización de la memoria: 30 días

2.3.1 Fase 1

Esta primera fase se realizó entre el 2 de febrero y el 25 de febrero. En esta primera fase se recolectó y seleccionó toda la documentación sobre GSM necesaria para realizar el trabajo. Además, se estudió a fondo esta documentación y se vieron pequeños ejemplos realizados en Matlab.

2.3.2 Fase 2

En esta segunda fase, el trabajo se centra en familiarizarse con las herramientas de trabajo. La primera parte de esta fase se dedica al aprendizaje del software LabVIEW. Para eso se realizan distintos tutoriales hechos por el fabricante y pequeñas pruebas. La segunda parte es para la familiarización con el hardware, realizando pequeñas pruebas con los transceptores y usando pequeños programas hechos con LabVIEW.

2.3.3 Fase 3

Esta tercera fase es la más importante del trabajo ya que en ella se realiza todo el grueso del proyecto. Los primeros días fueron para la comprobación de los módulos realizados por anteriores compañeros, mientras que, el resto del tiempo fue para la realización de todos los módulos necesarios para cumplir el objetivo del trabajo.

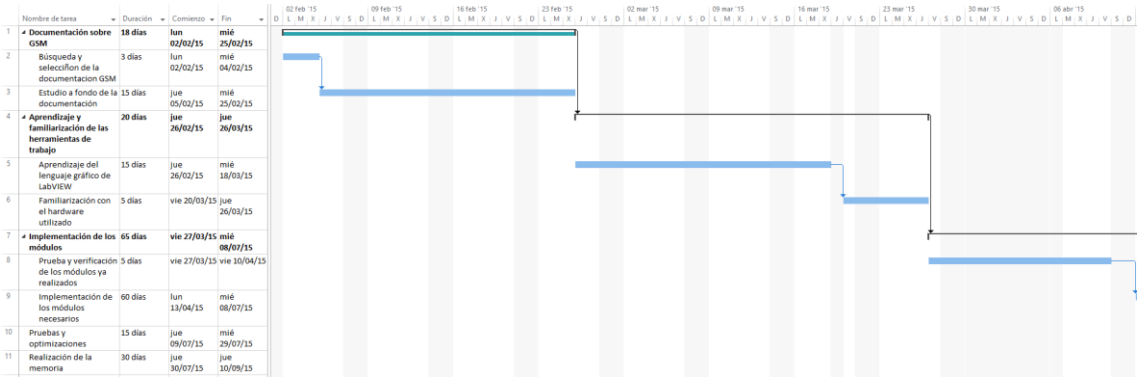
2.3.4 Fase 4

La fase cuatro se utilizó para realizar todas las pruebas a los módulos y al conjunto del trabajo. Esta fase de pruebas se realizó al finalizar los módulos pero gran parte de ella también se realizaba durante la programación.

2.3.5 Fase 5

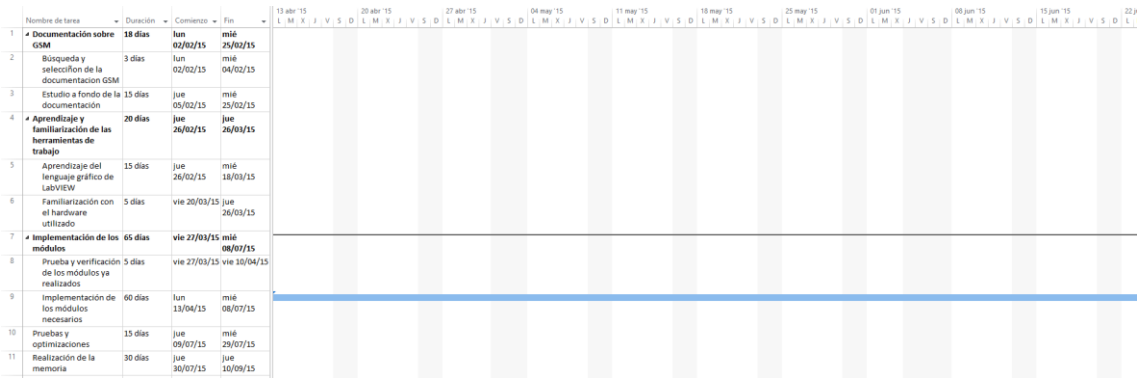
Por último, tras realizar todo el trabajo se procede a la escritura de la memoria.

A continuación se muestra un diagrama de Gantt para ver de forma más clara el orden seguido para realizar las tareas y las fechas en las que se realizaron.



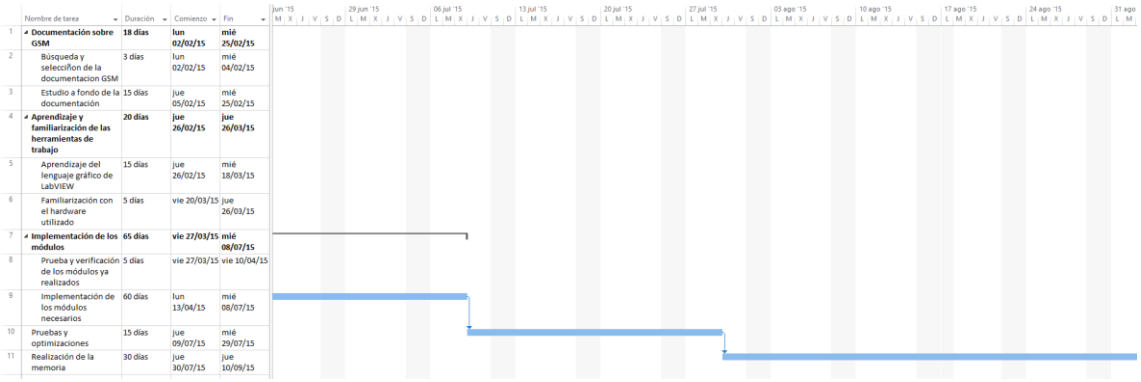
	Nombre de tarea	Duración	Comienzo	Fin
1	**Documentación sobre GSM**	**18 días**	**lun 02/02/15**	**mié 25/02/15**
2	Búsqueda y selecciñon de la documentacion GSM	3 días	lun 02/02/15	mié 04/02/15
3	Estudio a fondo de la documentación	15 días	jue 05/02/15	mié 25/02/15
4	**Aprendizaje y familiarización de las herramientas de trabajo**	**20 días**	**jue 26/02/15**	**jue 26/03/15**
5	Aprendizaje del lenguaje gráfico de LabVIEW	15 días	jue 26/02/15	mié 18/03/15
6	Familiarización con el hardware utilizado	5 días	vie 20/03/15	jue 26/03/15
7	**Implementación de los módulos**	**65 días**	**vie 27/03/15**	**mié 08/07/15**
8	Prueba y verificación de los módulos ya realizados	5 días	vie 27/03/15	vie 10/04/15
9	Implementación de los módulos necesarios	60 días	lun 13/04/15	mié 08/07/15
10	Pruebas y optimizaciones	15 días	jue 09/07/15	mié 29/07/15
11	Realización de la memoria	30 días	jue 30/07/15	jue 10/09/15

Figura 16: Cronograma (parte 1)



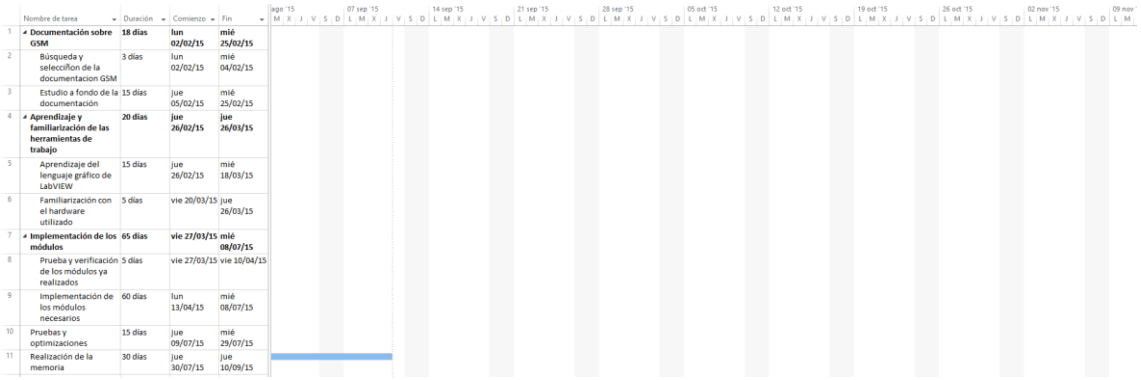
	Nombre de tarea	Duración	Comienzo	Fin
1	**Documentación sobre GSM**	**18 días**	**lun 02/02/15**	**mié 25/02/15**
2	Búsqueda y selecciñon de la documentacion GSM	3 días	lun 02/02/15	mié 04/02/15
3	Estudio a fondo de la documentación	15 días	jue 05/02/15	mié 25/02/15
4	**Aprendizaje y familiarización de las herramientas de trabajo**	**20 días**	**jue 26/02/15**	**jue 26/03/15**
5	Aprendizaje del lenguaje gráfico de LabVIEW	15 días	jue 26/02/15	mié 18/03/15
6	Familiarización con el hardware utilizado	5 días	vie 20/03/15	jue 26/03/15
7	**Implementación de los módulos**	**65 días**	**vie 27/03/15**	**mié 08/07/15**
8	Prueba y verificación de los módulos ya realizados	5 días	vie 27/03/15	vie 10/04/15
9	Implementación de los módulos necesarios	60 días	lun 13/04/15	mié 08/07/15
10	Pruebas y optimizaciones	15 días	jue 09/07/15	mié 29/07/15
11	Realización de la memoria	30 días	jue 30/07/15	jue 10/09/15

Figura 17: Cronograma (parte 2)



	Nombre de tarea	Duración	Comienzo	Fin
1	**Documentación sobre GSM**	**18 días**	**lun 02/02/15**	**mié 25/02/15**
2	Búsqueda y selecciñon de la documentacion GSM	3 días	lun 02/02/15	mié 04/02/15
3	Estudio a fondo de la documentación	15 días	jue 05/02/15	mié 25/02/15
4	**Aprendizaje y familiarización de las herramientas de trabajo**	**20 días**	**jue 26/02/15**	**jue 26/03/15**
5	Aprendizaje del lenguaje gráfico de LabVIEW	15 días	jue 26/02/15	mié 18/03/15
6	Familiarización con el hardware utilizado	5 días	vie 20/03/15	jue 26/03/15
7	**Implementación de los módulos**	**65 días**	**vie 27/03/15**	**mié 08/07/15**
8	Prueba y verificación de los módulos ya realizados	5 días	vie 27/03/15	vie 10/04/15
9	Implementación de los módulos necesarios	60 días	lun 13/04/15	mié 08/07/15
10	Pruebas y optimizaciones	15 días	jue 09/07/15	mié 29/07/15
11	Realización de la memoria	30 días	jue 30/07/15	jue 10/09/15

Figura 18: Cronograma (parte 3)



	Nombre de tarea	Duración	Comienzo	Fin
1	**Documentación sobre GSM**	**18 días**	**lun 02/02/15**	**mié 25/02/15**
2	Búsqueda y selecciñon de la documentacion GSM	3 días	lun 02/02/15	mié 04/02/15
3	Estudio a fondo de la documentación	15 días	jue 05/02/15	mié 25/02/15
4	**Aprendizaje y familiarización de las herramientas de trabajo**	**20 días**	**jue 26/02/15**	**jue 26/03/15**
5	Aprendizaje del lenguaje gráfico de LabVIEW	15 días	jue 26/02/15	mié 18/03/15
6	Familiarización con el hardware utilizado	5 días	vie 20/03/15	jue 26/03/15
7	**Implementación de los módulos**	**65 días**	**vie 27/03/15**	**mié 08/07/15**
8	Prueba y verificación de los módulos ya realizados	5 días	vie 27/03/15	vie 10/04/15
9	Implementación de los módulos necesarios	60 días	lun 13/04/15	mié 08/07/15
10	Pruebas y optimizaciones	15 días	jue 09/07/15	mié 29/07/15
11	Realización de la memoria	30 días	jue 30/07/15	jue 10/09/15

Figura 19: Cronograma (parte 4)

Como se aprecia en el diagrama de Gantt, el camino crítico recorre todas las tareas, debido a que para comenzar la siguiente fase del trabajo hay que realizar antes la anterior. Como excepción se podría destacar la fase de pruebas, que a pesar de que fue una etapa en sí misma al final del trabajo práctico, se fue realizando durante todo el proyecto.

A pesar de que en esta planificación aparecen muy diferenciadas las etapas, únicamente se muestra el tiempo que se ha dedicado exclusivamente a esa tarea. Durante la fase de implementación de los módulos se hicieron las primeras pruebas para ir comprobando el funcionamiento de estos y, tras la realización de los módulos, se dedicaron 15 días exclusivamente para ejecutar pruebas y optimizaciones.

3. Planteamiento del problema

3.1 Estado del arte

Las comunicaciones móviles son un entorno de trabajo muy extenso y en constante desarrollo. Es por eso que tecnologías radio definidas por software (SDR o Software Defined Radio) se convierten en una buena alternativa, ya que permitiría realizar dispositivos con menos hardware específico y que se puedan adaptar a las nuevas tecnologías que vayan surgiendo.

En el caso de los móviles, un terminal basado en una plataforma SDR, podría ser actualizado mediante software para adaptarse a nuevos estándares de comunicación que puedan surgir durante la vida útil del aparato.

Típicamente, una plataforma SDR puede estar formada por un adaptador de radio frecuencia, un conversor analógico-digital y un ordenador que se encargue de todo el procesamiento de la señal y de las operaciones necesarias.

Como se ha detallado anteriormente, en este trabajo se hace uso de una plataforma de programación como es LabVIEW y cuatro transceptores NI-USRP 2920, pero hay en el mercado herramientas, tanto software como hardware, para poder realizar el proyecto de forma distinta.

Estos USRP únicamente son fabricados por las empresas National Instruments y Ettus Research (propiedad de National Instruments), por lo que no hay alternativas similares para realizar el proyecto. A pesar de esto, los USRP podrían ser sustituidos por otros dispositivos como FPGAs, complicando su desarrollo y, en la mayoría de los casos, con peores características que estos transceptores.

Como alternativa a LabVIEW, una de las alternativas más potentes y usadas en SDR es GNU Radio. GNU Radio es un conjunto de herramientas gratuitas y de código libre que contienen bloques de procesado de señal para implementar en radios software. GNU Radio es compatible con la gran mayoría de transceptores que hay en el mercado (incluyendo los USRP usados).

La siguiente imagen muestra un ejemplo de la interfaz de usuario de GNU Radio:

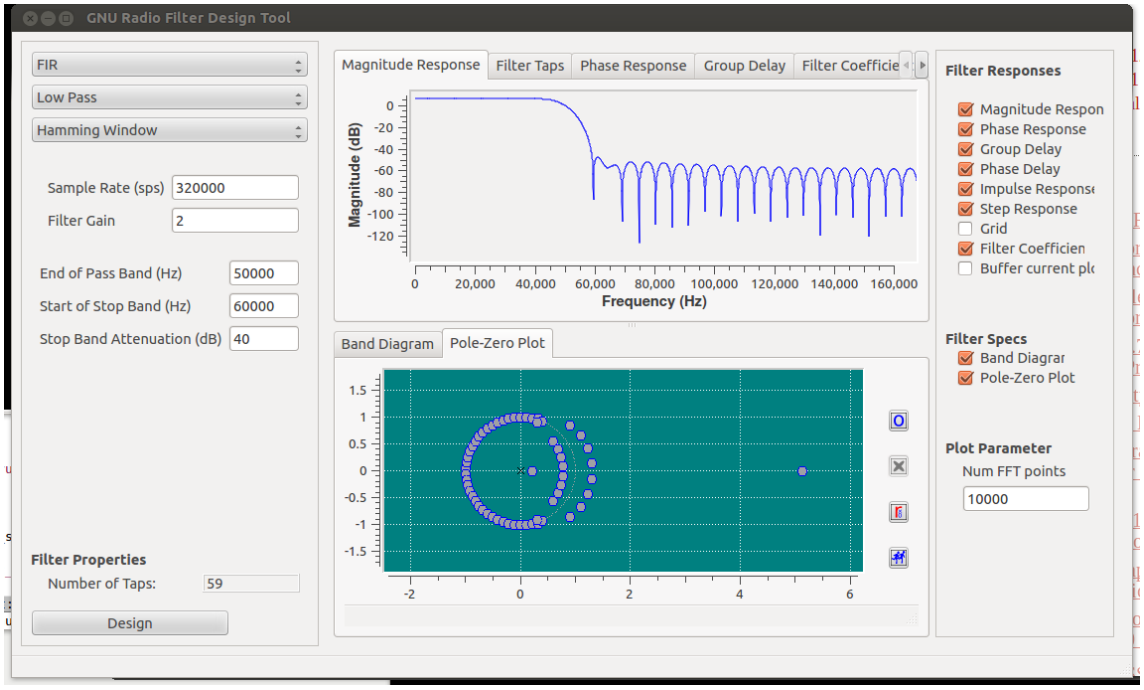


Figura 20: GNU Radio [4]

Otra herramienta utilizada en el mundo del SDR es SDR-RADIO.com. Esta herramienta, disponible para Windows, ofrece las funciones necesarias para trabajar con este tipo de plataformas. Además, al igual que GNU Radio, esta herramienta es gratuita y compatible con gran variedad de transceptores.

La siguiente imagen muestra un ejemplo de la interfaz de usuario de SDR-Radio.com:

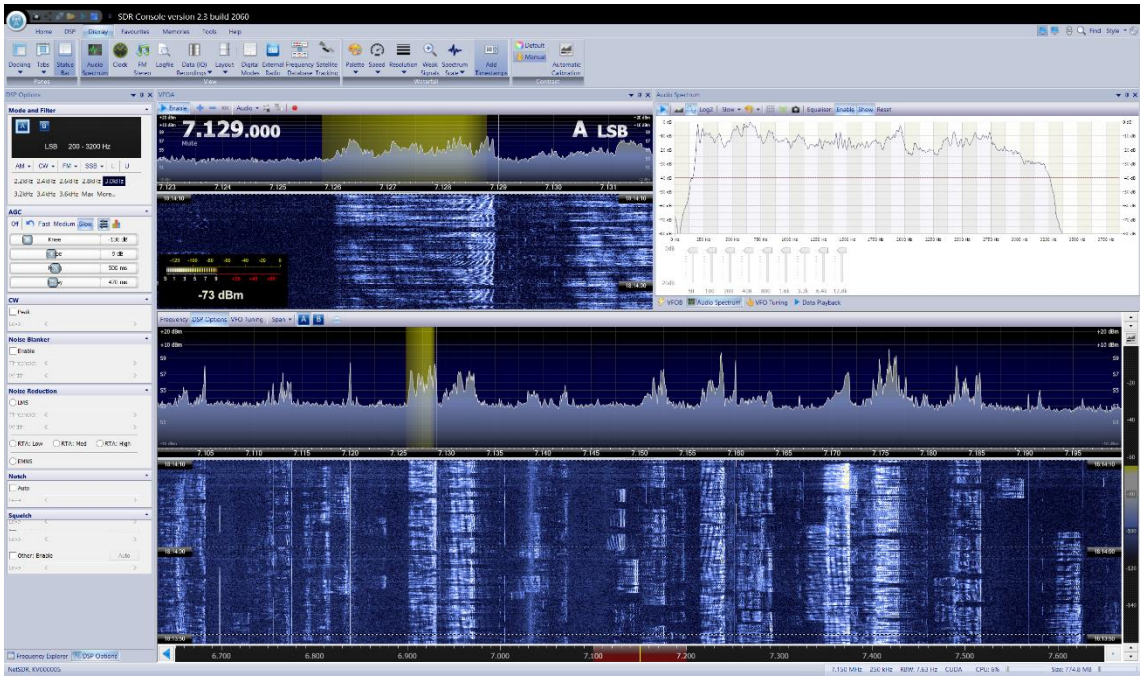


Figura 21: SDR-Radio.com [5]

A pesar de haber varios equipos que realicen funciones similares a las del objetivo de este trabajo no resta importancia ni a los equipos ni al trabajo. Los equipos en el laboratorio son limitados, aunque podrán seguir usándose para obtener mejores resultados que con este trabajo. Por otra parte, la gran finalidad de este proyecto no es la de realizar las funciones que puedan desarrollar esos equipos, si no de acercar a futuros alumnos esta tecnología y que puedan entender cómo funciona.

La elección de usar los USRP de National Instruments se debe a que son los transceptores disponibles en el laboratorio. Al usar estos USRP, lo lógico es usar el software LabVIEW proporcionado también por National Instruments, que, además, incluye ciertas funcionalidades para estos transceptores.

3.2 Marco regulador

El marco regulador más importante en materias de telecomunicaciones es la nueva Ley General de Telecomunicaciones 9/2014 [6]. Esta ley se divide en ocho títulos:

Título I. Disposiciones generales.
Título II. Explotación de redes y prestación de servicios de comunicaciones electrónicas en régimen de libre competencia.
Título III. Obligaciones de servicio público y derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas.
Título IV. Evaluación de la conformidad de equipos y aparatos.
Título V. Dominio público radioeléctrico.
Título VI. La administración de las telecomunicaciones.
Título VII. Tasas en materia de telecomunicaciones.
Título VIII. Inspección y régimen sancionador.

A pesar de la gran cantidad de aspectos que regula esta ley, a este trabajo solo le afecta lo relacionado con emisiones radioeléctricas y la evaluación de equipos, es decir los títulos IV y V de la Ley General de Telecomunicaciones.

A continuación se presentan los artículos más relacionados con este trabajo que contiene este título IV con una breve explicación:

- **Artículo 56:** Donde se indica que las características de las redes y aparatos se regularán mediante Real Decreto.
- **Artículo 57:** Todos los equipos deberán ser evaluados conforme a la normativa vigente antes de su uso.

- **Artículo 58:** Los equipos que se hayan evaluado dentro de la Unión Europea o mediante acuerdos con terceros serán válidos para su uso en España.

En cuanto al título V de la Ley General de Telecomunicaciones, en él se indica que el espectro radioeléctrico es un bien de dominio público cuya titularidad corresponde al Estado Español y que será éste el que lo controle y gestione.

Por otra parte, el Real Decreto 1066/2001 [7] establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas. En el cuadro 1 de este Real Decreto se obtienen unos límites para frecuencias entre 10 MHz y 10 GHz de:

- SAR medio de cuerpo entero: 0,08 W/kg.
- SAR localizado (cabeza y tronco): 2 W/kg.
- SAR localizado (miembros): 4 W/kg.

Por último, al ser un trabajo académico sin fines de usar los resultados fuera de ésta, el trabajo no tiene restricciones legales destacadas, aunque, como todas las obras, está sujeta a la Ley de Propiedad Intelectual, que concede un conjunto de derechos a los autores y otros titulares de las obras.

3.3 Marco socioeconómico

Debido a la finalidad didáctica de este trabajo, el entorno socioeconómico no afecta a éste de manera directa.

Por el contrario, este trabajo si puede afectar al marco socioeconómico del país. A causa de la finalidad docente del trabajo, ayudará a mejorar la docencia y la formación de futuros estudiantes de grados de telecomunicaciones. Esto, a su vez, ayudará que en España, tanto la investigación como el desarrollo de posibles productos se verán reforzados. Por tanto, debido a la importancia del sector de la tecnología en general y de las TIC en particular, mejorar la investigación en este campo redundará en la economía del país, creando mayor riqueza.

En el capítulo 7 de este trabajo se presenta un presupuesto detallado en el que se incluyen todos los costes del proyecto.

4. Estándar GSM

4.1 Introducción

GSM se inicia como un proyecto para realizar un sistema de comunicaciones móviles global. El estándar se comenzó a desarrollar en 1982 y en el año 1990 ya se presentaron las primeras especificaciones de GSM-900.

Con GSM se querían conseguir algunas características importantes como:

- Buena calidad de voz, cobertura y capacidad.
- Bajo coste.
- Sistema global para poder usar tú móvil en otros países (roaming).
- Interoperabilidad de equipos.
- Eficiencia espectral.
- Compatibilidad con otras redes (ISDN, PSTN, etc).

Para cumplir esas características, se decidió utilizar un sistema digital de comunicaciones con una red celular.

4.2 Diseño celular

Para cumplir los requisitos de GSM (utilización eficiente del espectro, buena cobertura, gran capacidad, etc) se decide realizar un diseño celular de la red.

En una red celular se divide toda la zona de cobertura en zonas menores llamadas celdas. Estas celdas pueden compartir frecuencias siempre que estén a una distancia suficiente para no producir interferencias notables. Además de celdas, existen las agrupaciones, que consisten en uniones de celdas que utilizan distintas frecuencias. La siguiente imagen muestra las celdas hexagonales y las agrupaciones, formadas por celdas que no comparten ninguna frecuencia:

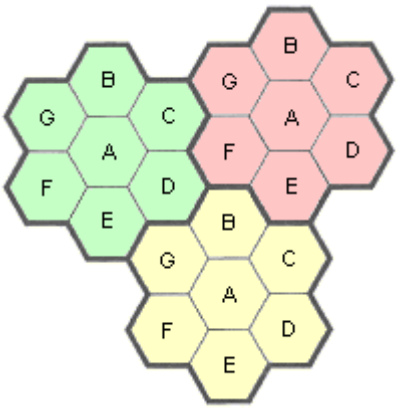


Figura 22: Ejemplo de diseño celular [8]

Además, en entornos con mucho tráfico como las ciudades se suele realizar sectorización. La sectorización consiste en colocar una antena directiva en el centro de la celda de modo que tenga un diagrama de radiación de 120º, pudiendo dividir la celda en tres zonas. De esta forma las interferencias disminuyen gracias a la directividad de las antenas. La siguiente figura muestra cómo se realiza la sectorización:

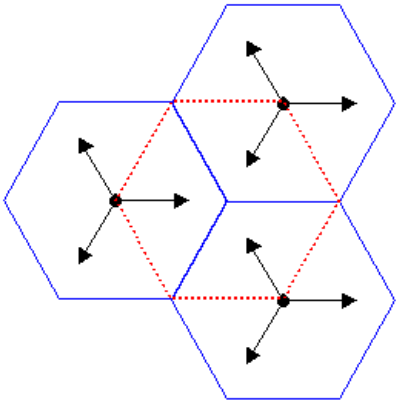


Figura 23: Sectorización [9]

La planificación celular es uno de los aspectos más importantes en GSM. Elegir el tamaño idóneo de las celdas y las agrupaciones es clave para mantener un equilibrio entre capacidad, interferencias y uso eficiente del espectro (a mayor tamaño de agrupación menor será la capacidad y menos eficientemente se utilizará el espectro pero las interferencias entre celdas será más baja).

En la planificación celular se intentará cubrir toda la zona de cobertura sin que haya solapes entre celdas. Para cumplir este objetivo sólo se pueden usar ciertas formas geométricas como triángulos, cuadrados y hexágonos. En GSM la planificación celular usa hexágonos, debido a que es la forma que permite cubrir más área con el mismo radio.

4.3 Especificaciones

4.3.1 Funcionalidad

La red GSM está diseñada para soportar las siguientes funcionalidades [3]:

1. Servicios básicos:
   1.1. Establecimiento de llamadas.
   1.2. Autenticación de usuarios y equipos.
   1.3. Encriptación de llamadas.
   1.4. Llamadas de emergencia.

2. Movilidad:
   2.1. Localización y registro de abonados.
   2.2. Itinerancia.
   2.3. Radiobúsqueda.
   2.4. Traspasos.
   2.5. Incorporación y abandono de la red.
3. Gestión de red:
   3.1. Operación y mantenimiento
   3.2. Gestión de abonados.
4. Gestión de recursos radio:
   4.1. Asignación de frecuencias.
   4.2. Mediciones de señal.

4.3.2 Servicios

En GSM hay dos fases de introducción de servicios. En una primera fase se introducirán los servicios más importantes para, después, en la segunda fase, añadir otros servicios más avanzados.

4.3.2.1 Teleservicios

En una primera fase se ofrecen los servicios de telefonía FS (Full Speed) a 13kbps, llamadas de emergencia y mensajes cortos (SMS) tanto punto a punto como de punto a multipunto o CBS (Cell Broadcast SMS).

En la segunda fase se añaden otros servicios como son la telefonía HS (Half Speed) a 6,5kbps y el SMS mejorado.

4.3.2.2 Servicios portadores

En cuanto a servicios portadores, en un principio se introdujeron los siguientes servicios:

- Datos asíncronos en modo circuito con velocidades de entre 300 y 9600 bps y dúplex.
- Datos síncronos en modo circuito con velocidades de entre 300 y 900 bps y dúplex.
- Acceso PAD (Packet Assembly - Disassembly) asíncrono con velocidades de enre 300 y 9600 bps.

Más tarde se añadirán, también, acceso PAD dedicado y acceso en modo paquete dedicado síncrono con velocidades de entre 2400 y 9600 bps.

4.3.2.3 Servicios suplementarios

Los servicios suplementarios en la primera fase eran pocos y estaban centrados en el tratamiento de llamadas entrantes o salientes como reencaminamiento, desvío o restricción de llamadas.

Sin embargo, en la segunda fase, los servicios suplementarios añadidos son numerosos [3]:

- Identificación de línea llamante.
- Restricción de identidad llamante.
- Llamada en espera.
- Retención de llamada.
- Multiconferencia.
- Grupo cerrado de usuarios.
- Aviso de tarificación.
- Servicios suplementarios no estructurados.
- Restricción de servicios por el operador.

4.4 Arquitectura de red

Debido a la estructura celular de la red y las funcionalidades que debe cumplir, la arquitectura de la red GSM es bastante compleja. Para reducir su complejidad, la arquitectura de la red se divide en subsistemas según su funcionalidad, tal y como indica la siguiente figura:

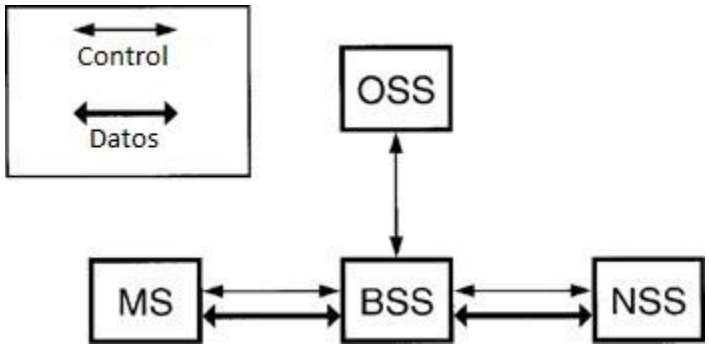


Figura 24: Arquitectura de red [26]

4.4.1 Mobile Station

En GSM la estación móvil está formada por dos elementos tal y como indica la figura 25:

- **Tarjeta SIM (Subscriber Identity Module):** se trata de una tarjeta inteligente en la que se almacena información relacionada con el usuario como números identificativos, claves y algoritmos.
- **Equipo móvil:** se trata del equipo que realiza las funciones de transmisión y recepción y de procesado de señal.

Figura 25: Terminal GSM y tarjeta SIM [27]

Las funciones más importantes de la estación móvil de GSM son:

- Comunicación entre el usuario y la red radio.
- Transmisión y recepción de información del usuario y señalización.
- Iniciar la conexión con la red.
- Sintonización de frecuencias y seguimiento de las estaciones base.
- Procesado de la voz.
- Adaptación entre distintas interfaces.

4.4.2 Base Station Subsystem

El subsistema de estación base está formado por las BTS y por las BSC. Una BSC puede controlar varias BTS mientras que, una BTS solo puede ser controlada por una única BSC.

Las BTS contienen los transceptores necesarios para realizar la transmisión y recepción de las señales. Las BSC, por su parte, son las encargadas de controlar varios BTS, gestionando recursos como frecuencias y conectando con el MSC.

El BSS tiene la siguiente estructura:

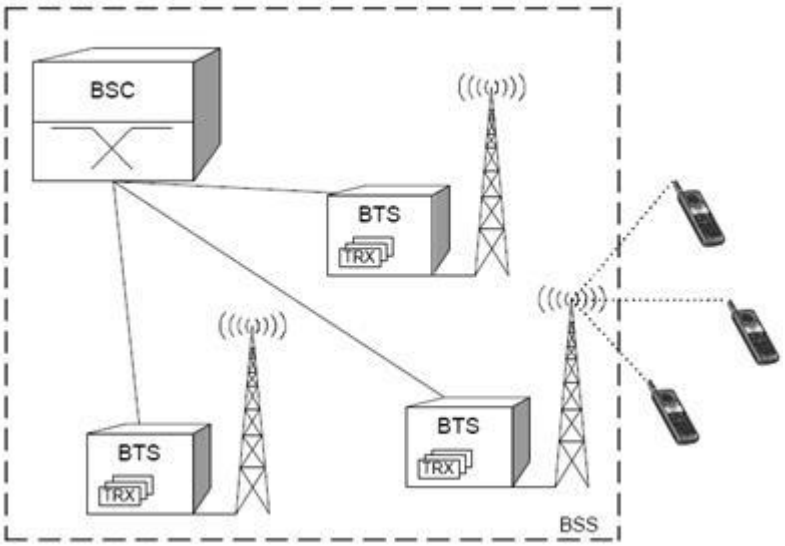


Figura 26: Base Station Subsystem [10]

El BSS tiene como funciones principales:

- Transmisión y recepción de las señales.
- Localización de la estación móvil.
- Establecer, supervisar y terminar llamadas.
- Procesar la voz y adaptar velocidades.
- Control de equipos.
- Control de mantenimiento.

4.4.3 Network Switching Subsystem

El subsistema de red conforma el núcleo de la red y está compuesto de varios elementos:

- **Central de conmutación móvil o MSC:** se comporta como una central telefónica encaminando llamadas aunque tiene otras funciones adicionales como procedimientos de localización y traspaso o gestión de llamadas.
- **Registro Base de Abonados o HLR:** base de datos que almacena a todos los clientes de un operador. En él se encuentran datos permanentes que identifican al usuario y otros datos temporales como la MSC visitada o la dirección del VLR en el que está registrado el usuario. El HLR es único por cada operador.

- **Registro de Abonados Visitantes o VLR:** base de datos en la que se almacena información de usuarios que usan esa MSC. Todo abonado conectado a la red debe estar inscrito en alguna VLR.
- **Centro de Autentificación o AuC:** proporciona al HLR la información necesaria para la autentificación en la red, guardando las identidades IMSI y la clave secreta de cada usuario.
- **Base de datos de equipos o EIR:** contiene tres listas con las que se identifica si el equipo puede o no puede usar la red.
    - *Lista blanca:* equipos aceptados.
    - *Lista gris:* equipos que pueden usar la red pero a los que es necesario localizar.
    - *Lista negra:* equipos que no pueden usar la red.

El subsistema de red tiene la siguiente estructura:

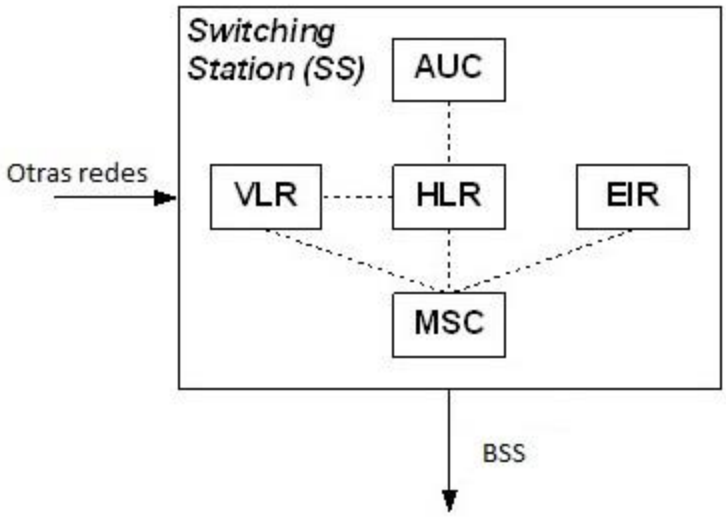


Figura 27: Network Switching Subsystem [11]

4.4.4 Operation Support Subsystem

El subsistema de operación y mantenimiento se encarga de la gestión de la red. Está formado por dos elementos:

- **Centro de operación y mantenimiento u OMC:** se encarga de las funciones de gestión técnicas o administrativas de la red.
- **Centro de gestión de red o NMC:** funciones similares al OMC pero de carácter más general.

4.5 Interfaz radio

La interfaz radio de cualquier red móvil es una de las partes más importantes, ya que de su correcto funcionamiento depende toda la red. En el caso de GSM, esta interfaz se identifica por el nombre Um y presenta unas características que se deben cumplir para que toda la red funcione correctamente

4.5.1 Acceso

La interfaz radio de GSM combina acceso por división en el tiempo (TDMA) con acceso por división en frecuencia (FDMA/FDD), ya que en la frecuencia de subida y de bajada es distinta y, a su vez, esas frecuencias se comparten por división en el tiempo.

En cuanto a la tecnología FDMA, en GSM el ancho de banda se divide en radiocanales de 200 kHz cada uno. A su vez, cada radiocanal se comparte mediante acceso TDMA, ya que está formado por ocho intervalos de tiempo llamados time slots. Cada time slot tiene una duración de 0.577 ms, por lo que la trama completa que forman los ocho intervalos de tiempo dura 4,615 ms. Además, en GSM se utiliza una tecnología FDD en la que el enlace de subida y de bajada están en distintas frecuencias y en distintos tiempos.

La siguiente figura muestra el desplazamiento de slots entre subida y bajada:

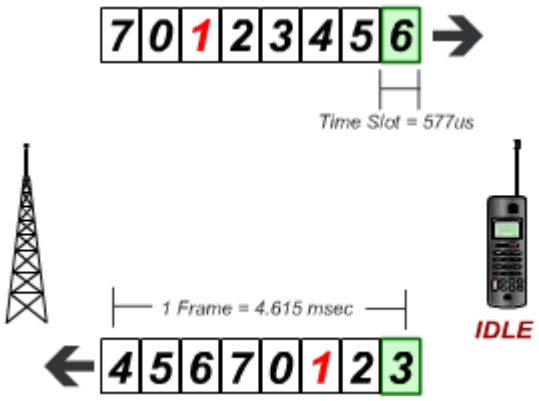


Figura 28: Desplazamiento de time slots [11]

En GSM-900 se dispone de la banda de 890-960 MHz. Para el enlace de subida se usan las frecuencias de 890-915 MHz y para el de bajada las de 935-960 MHz, habiendo una diferencia de 45 MHz entre el enlace de bajada y de subida. Además de la diferencia de frecuencia entre dichos enlaces, hay una diferencia de tiempo de 3

slots (el enlace de subida va retrasado 3 time slots con respecto al de bajada) para que el móvil no tenga que enviar y recibir en el mismo tiempo.

4.5.2 Ráfagas

Los time slots mencionados anteriormente contienen información estructurada en ráfagas. Cada una de estas ráfagas tiene distintos campos según su utilidad y distinta información útil.

4.5.2.1 Normal Burst

La ráfaga Normal Burst contiene los siguientes campos:

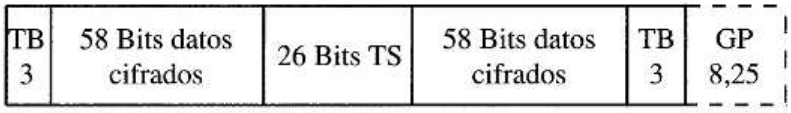


Figura 29: Normal Burst [2]

La normal burst es la ráfaga más utilizada. Se usa para canales de tráfico y de control (exceptuando el canal RACH)

4.5.2.2 Frequency Correction Burst

La ráfaga Frequency Correction Burst contiene los siguientes campos:

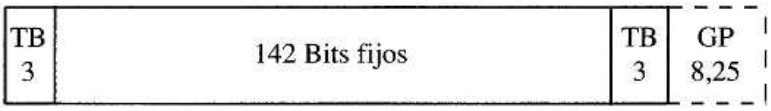


Figura 30: Frequency Correction Burst [3]

La ráfaga de corrección de frecuencia se utiliza para la sincronización del móvil. Los 142 bits fijos producen un tono conocido al modularse, lo que hace que, el móvil al detectarlo, pueda sincronizarse en frecuencia.

4.5.2.3 Synchronization Burst

La ráfaga de sincronización contiene los siguientes campos:

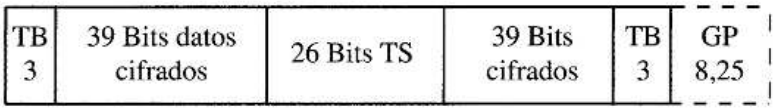


Figura 31: Synchronization Burst [3]

La ráfaga de sincronización se utiliza para la sincronización en tiempo del móvil. Ésta se produce al detectar los 26 bits de la training sequence en el móvil. Además,

en esta ráfaga se introducen datos importantes de la BSS, como el BSIC o el reloj actual de la BTS.

4.5.2.4 Dummy Burst

La ráfaga Dummy Burst contiene los siguientes campos:

Figura 32: Dummy Burst [3]

La ráfaga de relleno se utiliza cuando la estación base no tiene canales de tráfico para transmitir.

4.5.2.5 Access Burst

La ráfaga de acceso contiene los siguientes campos:

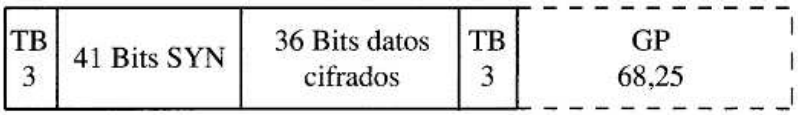


Figura 33: Access Burst [3]

La ráfaga de acceso se utiliza para el acceso aleatorio a través del canal RACH. Los 41 bits de sincronización se utiliza para que el BSS detecte donde comienza la ráfaga de acceso.

4.5.3 Canales

En GSM se distinguen dos tipos de canales: canales físicos y canales lógicos.

4.5.3.1 Canales físicos

Los canales físicos vienen determinados por el número de time slot y frecuencia utilizada, es decir, este tipo de canal no depende del tipo de información que se envía, si no que depende únicamente de donde se envía esa información.

4.5.3.2 Canales lógicos

Los canales lógicos, a diferencia de los físicos, sí dependen de la información. Existen varios tipos de canales lógicos [12].

1. Canales de tráfico:
   1.1. TCH/F: Canal de tráfico a velocidad total (13 kbps en voz y 9,6 kbps en datos).

1.2. TCH/H: Canal de tráfico a velocidad mitad (6,5 kbps en voz y 4,8 kbps en datos).

2. Canales de control comunes: canales de difusión y de control comunes para regular el acceso al sistema.
   2.1. BCH (Broadcast Control Channels): canales de bajada (de BTS a estación móvil) que envían información general de la red GSM.
      2.1.1. BCCH (Broadcast Common Control Channel): información general de la estación base y de otros canales de control.
      2.1.2. FCCH (Frequency Correction Channel): señal piloto para ajuste de frecuencia en los terminales móviles.
      2.1.3. SCH (Synchronization Channel): identificación de la BTS y sincronización en tiempo del terminal móvil.
   2.2. CCCH (Common Control Channels): canales para transmitir información desde la red a los terminales y para darles acceso.
      2.2.1. RACH (Random Access Channel): canal de subida por el que se cursan peticiones no programadas. Utiliza ALOHA ranurado.
      2.2.2. PCH (Paging Channel): canal de bajada por el que se notifica una llamada entrante a un terminal móvil.
      2.2.3. AGCH (Access Grant Channel): canal de bajada por el que se asignan otros canales a una estación móvil.
   2.3. DCCH (Dedicated Control Channels): canales de subida y bajada con señalización relacionada con una llamada.
      2.3.1. SDCCH (Stand Alone Dedicated Control Channel): canal para intercambiar datos entre el terminal móvil y la BTS antes de tener asignado un TCH.
      2.3.2. SACCH (Slow Associated Control Channel): señalización lenta asociada a la llamada en curso.
      2.3.3. FACCH (Fast Associated Control Channel): señalización de órdenes urgentes.
   2.4. CBCH (Cell Broadcast Channel): difusión de mensajes cortos desde una célula.

4.5.4 Multiacceso

Para simplificar el sistema, GSM utiliza una jerarquía de acceso de la siguiente manera:

- Un conjunto de 8 slots forman una trama (4,165 ms).
- Una multitrama puede estar formada por 26 tramas si son canales de datos (MF26) o por 51 tramas si son canales de control (MF51).
- Una supertrama se compone de 51 MF26 o de 26 MF51.
- Por último, existe la hipertrama, que se compone de 2048 supertramas.

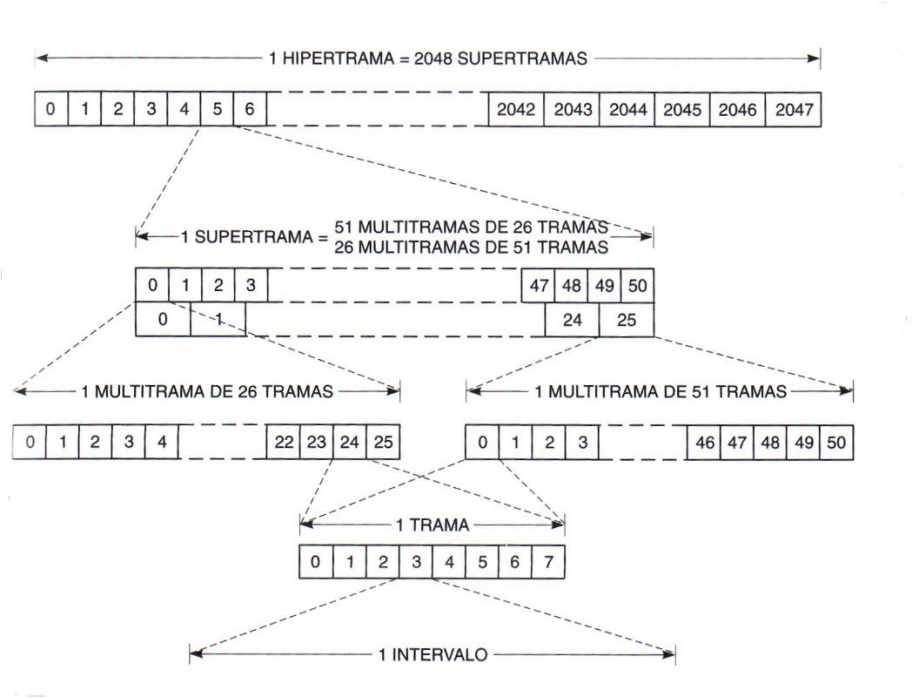


Figura 34: Multiacceso en GSM [12]

4.5.5 Procesado en banda base

Para adecuar la señal al canal radio se realizan una serie de procedimientos [3]:

1. **Codificación de fuente** (únicamente para canales de voz):
   - Se utiliza para minimizar la información que se envía manteniendo la calidad por encima de un umbral.
   - Se usa una codificación predictiva lineal: RDP-LTP (Regular Pulse Excited – Long Term Prediction)
2. **Codificación de canal:**
   - El objetivo es detectar y corregir errores.
   - En GSM las técnicas más utilizadas son: códigos bloque y convolucional para corregir errores, códigos FIRE para detección y corrección y códigos de paridad para detección.
   - Tras la codificación de canal típicamente resultan 456 bits.

3. **Entrelazado:**
    - Consiste en distribuir los bits para que errores producidos en el canal no afecten a bits consecutivos.

4.5.6 Identificación y números de abonado y red

En GSM existen números que permiten la identificación del abonado y de la red [3]:

1. **IMSI (International Mobile Subscriber Identity):** identifica al usuario a nivel internacional y está en la SIM. Este número, por razones de seguridad, solo se utiliza en el primer acceso a la red, en los siguientes se usa el TMSI, que se trata de un número temporal.
2. **MS-ISDN (Mobile Station ISDN):** es el número de teléfono del abonado.
3. **IMEI (International Mobile Equipment Identity):** identifica al terminal móvil.
4. **MSRN (Mobile Subscriber Roaming Number):** se usa en el encaminamiento a la PSTN.

4.5.7 Modulación

La modulación utilizada en GSM es una variación de la MSK, llamada GMSK. Este tipo de modulación tiene las ventajas de la MSK como la envolvente constante, el uso de un modulador sencillo, ancho de banda bajo y a su vez soluciona uno de sus grandes problemas que es la radiación en bandas adyacentes. A pesar de las grandes ventajas de esta modulación tiene el problema de que produce ISI (Interferencia Inter Simbólica).

La modulación en GSM consta de las siguientes etapas [13]:

1. **Codificación diferencial**

Cada bit de entrada se codifica diferencialmente según la expresión:

$$\widehat{d}_i = d_i \oplus d_{i-1}$$

Ecuación 1: Codificación diferencial

Los valores que entran al modulador vienen definidos por:

$$\alpha_i = 1 - 2\widehat{d}_i$$

Ecuación 2: Valores de entrada al modulador

2. Filtrado

Los datos codificados representados como pulsos de Dirac excitan un filtro lineal con respuesta al impulso definida por:

$$g(t) = h(t) * rect\left(\frac{t}{T}\right)$$

Ecuación 3: Respuesta al impulso

Donde la función rect viene definida por:

$$rect\left(\frac{t}{T}\right) = \begin{cases} \frac{1}{T}, & |t| < \frac{T}{2} \\ 0, & en\ otro\ caso \end{cases}$$

Ecuación 4: Función rect

Y h(t):

$$h(t) = \frac{\exp(\frac{-t^2}{2\delta^2 T^2})}{\sqrt{2\pi}\delta T}$$

Ecuación 5: Expresión de h(t)

con:

$$\delta = \frac{\sqrt{\ln(2)}}{2\pi BT}\ y\ BT = 0{,}3$$

Ecuación 6. Valor de delta

3. Fase de salida

La fase de la señal modulada es:

$$\varphi(t') = \sum_i \alpha_i\, \pi h \int_{-\infty}^{t'-iT} g(u)\, du$$

Ecuación 7: Fase de la señal modulada

El valor de h es ½.

4. Modulación

Finalmente, la señal modulada tendría la siguiente expresión:

$$x(t') = \sqrt{\frac{2E_c}{T}} \cos 2\pi f_0 t' + \varphi(t') + \varphi_0$$

Ecuación 8: Expresión de la señal modulada

Donde Ec s la energía por bit, f0 la frecuencia central de la portadora y φ_0 una fase aleatoria.

5. Entorno de trabajo

5.1 Hardware utilizado

5.1.1 NI USRP-2920

Los transceptores NI USRP-2920 son los encargados de recibir y enviar las señales. Estos transceptores utilizan el software LabVIEW y son muy utilizados en laboratorios, tanto para pruebas como para propósito didáctico. La siguiente imagen muestra el aspecto de un USRP-2920.

Figura 35: Transceptor NI USRP 2920 [28]

Las conexiones utilizadas en este trabajo son:

- Entrada de la fuente de alimentación.
- Puerto Gigabit Ethernet: para la conexión con el ordenador.
- Entradas para antenas: TX1/RX1 y RX2. En este trabajo solo se utiliza una antena por USRP por lo que se conecta a la entrada TX1/RX1.
- Entrada MIMO: para conectar dos USRP entre sí. En este trabajo se utiliza para unir entre sí los dos USRP que actúan de BTS y los dos USRP de la estación móvil.

El panel frontal donde se realizan las conexiones del USRP es el siguiente:

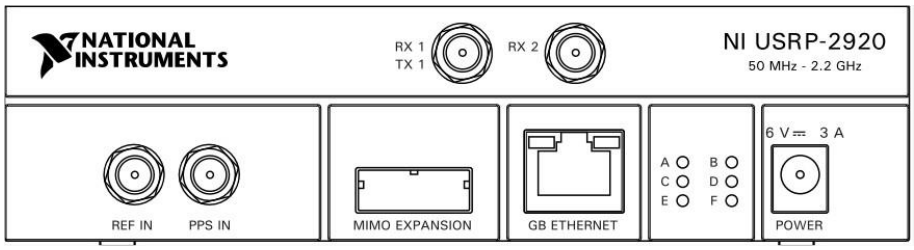


Figura 36: Panel frontal del transceptor [28]

Algunas características de estos transceptores y las que más afectan a este trabajo son:

- Rango de frecuencia: de 50 MHz a 2,2 GHz. En este TFG se usa la frecuencia de 600 MHz por ser una de las bandas con menos interferencias.
- Potencia máxima de transimisión: entre 15 y 20 dBm.
- Ancho de banda: hasta 20 MHz. En el trabajo se usa un ancho de banda de 200 KHz (1 portadora GSM).
- Número de muestras: hasta 400 MS/s (megamuestras por segundo).

El hardware del USRP funciona según el siguiente esquema:

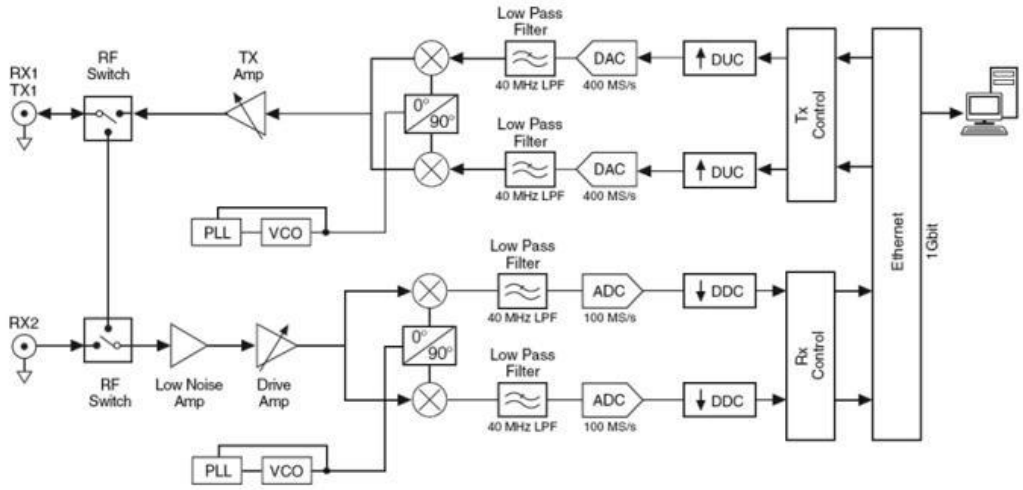


Figura 37: Esquema del hardware del transceptor [14]

5.2 LabVIEW

Para programar las funcionalidades descritas anteriormente se eligió el software LabVIEW (Laboratory Virtual Instrumentation Engineering Workbench), una plataforma muy útil para ingenieros con una gran cantidad de herramientas disponibles.

LabVIEW fue creada por National Instruments y su primera versión fue en el año 1986, únicamente para maquinas MAC. Actualmente, su última versión es del 2014 y funciona tanto en máquinas MAC como en Windows, UNIX y GNU/LINUX.

La principal característica de LabVIEW es su estilo de programación que, a diferencia de los lenguajes de programación habituales como Java o C, se trata de una programación gráfica en la que se utilizan iconos con distintas funcionalidades y parámetros de entrada y de salida para componer el programa final. La siguiente figura muestra un ejemplo de este tipo de programación gráfica:

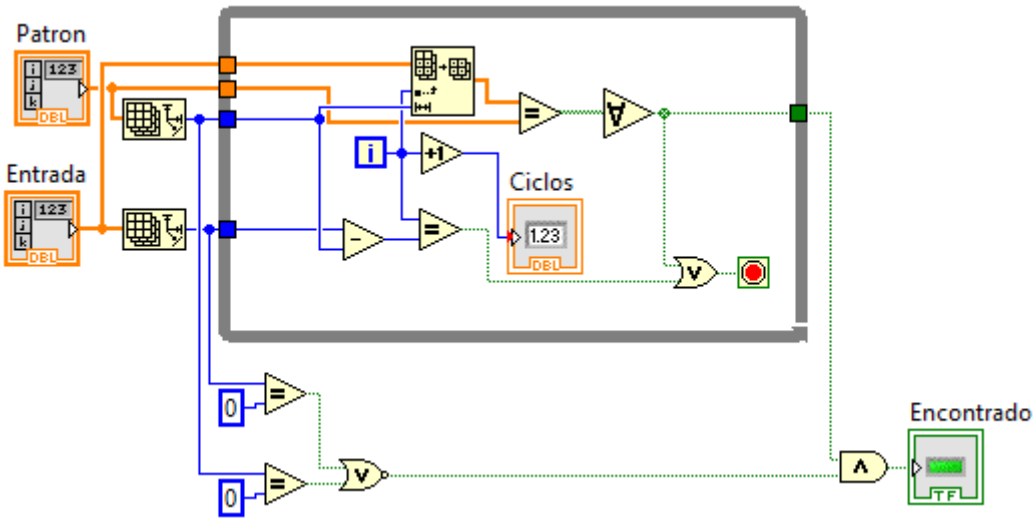


Figura 38: Ejemplo de programación gráfica

Los programas creados con LabVIEW se llaman instrumentos virtuales (VI o Virtual Instruments). Cada VI se compone de dos partes:

1. **Panel frontal:** el panel frontal hace de interfaz para el usuario. Está formado por controles e indicadores. Con los controles el usuario puede controlar la ejecución del programa modificando sus entradas, mientras que con los segundos el programa puede mostrar al usuario distintas salidas. El panel frontal en LabVIEW tiene el siguiente aspecto:

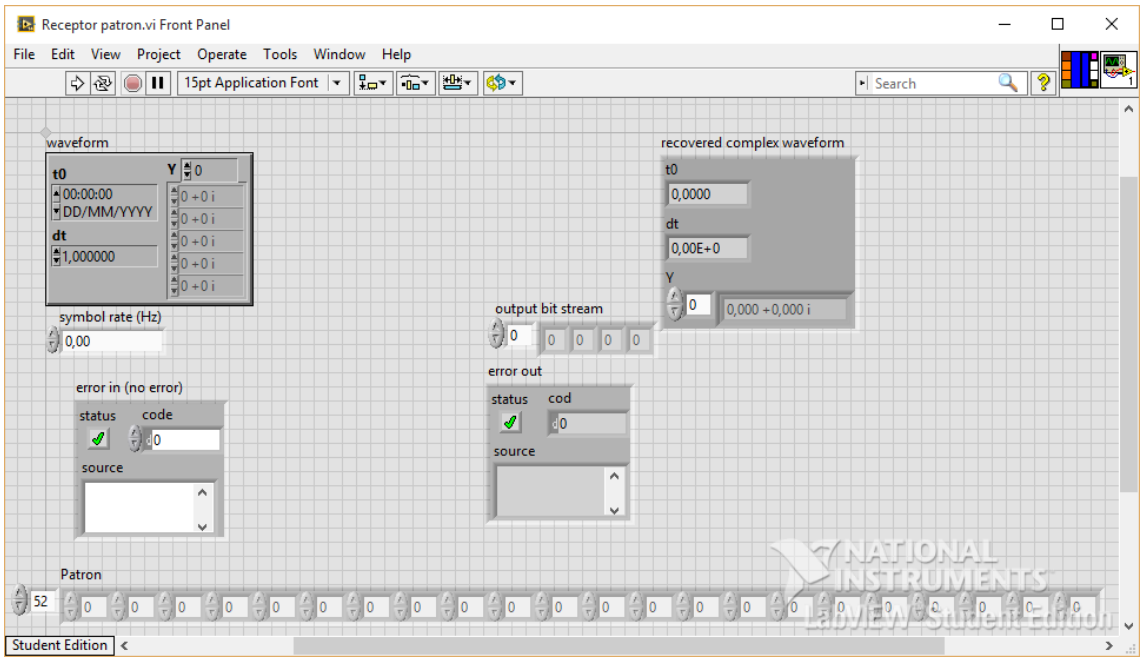


Figura 39: Panel frontal

2. **Diagrama de bloques:** es el conjunto de iconos y otros VI que forman el programa propiamente dicho. La siguiente imagen muestra un ejemplo de diagrama de bloques en LabVIEW:

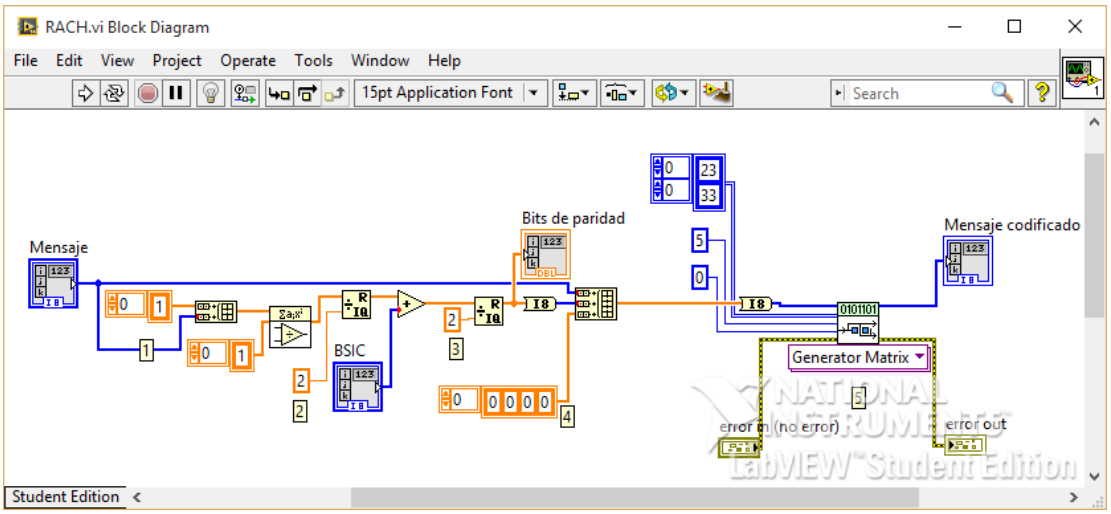


Figura 40: Diagrama de bloques

5.2.1 Ordenadores portátiles.

Para el desarrollo del trabajo se ha utilizado como ordenador principal un portátil ASUS A55A con las siguientes características:

- Procesador Intel Core i7 de 8 núcleos a 2,4 GHz.
- Memoria RAM DDR3 de 8GB.
- Disco duro de 500 GB.
- Tarjeta GigabitEthernet.
- Tarjeta gráfica Intel HD Graphics 4000.
- Sistema operativo Windows 8.1 con una arquitectura de 64bits.

Este ordenador se utilizó para programar en lenguaje LabVIEW y para pequeñas pruebas que se podía realizar con un único ordenador.

Para la puesta en marcha de los transceptores y las pruebas se ha utilizado un segundo ordenador portátil Acer TavelMate 5760 con estas características:

- Procesador Intel Core i3 a 2,1 GHz.
- Memoria RAM DDR3 de 6GB.
- Disco duro de 500 GB.
- Tarjeta GigabitEthernet.

- Tarjeta gráfica nVidia GT 540M.
- Sistema operativo Windows 7 con arquitectura de 64 bits.

5.2.2 Agilent VSA 89600S

Este analizador vectorial de señales desarrollado por Agilent consta de dos partes, una hardware encargada de recibir señales y otra software encargada de analizarlas. Este analizador además de ser capaz de analizar señales GSM, sirve para muchos más estándares como WiFi o UMTS. En la siguiente imagen se muestra la parte hardware del analizador (parte de la derecha) y la parte software controlada con el ordenador (parte de la izquierda).

Figura 41: Agilent VSA 89600S [15]

Este equipo se utiliza para realizar pequeñas pruebas durante el proceso de diseño del proyecto y para las comprobaciones de funcionamiento finales.

6. Diseño y desarrollo

El objetivo principal de este proyecto es realizar una implementación del procedimiento de attach en GSM en una plataforma Software Defined Radio utilizando transceptores USRP.

En GSM el procedimiento de attach se realiza cuando se enciende el móvil y se intenta conectar a una BTS. El móvil tiene que pedir un canal para enviar cierta información de autenticación que luego la red GSM comprueba para conceder o denegar el acceso a esa red.

Para conseguir ese objetivo hay que realizar una serie de módulos y funciones:

- Realizar una implementación de los canales RACH, SDCCH y AGCH con sus respectivas codificaciones y decodificaciones.
- Desarrollar módulos que tengan como salida los mensajes necesarios para realizar el procedimiento.
- Desarrollar módulos para la transmisión y recepción de estos mensajes, incluyendo la modulación GMSK usada en GSM.
- Realizar una interfaz para que el usuario pueda interactuar con el programa.

Debido a problemas con el modulador y limitaciones con los transceptores NI-USRP, la sincronización no se realiza de la forma en la que se realiza en GSM, si no que los mensajes son detectados por la secuencia de entrenamiento en el caso de los canales AGCH y SDCCH y por los bits de sincronización en el caso del canal RACH.

Para realizar la implementación de todo el proyecto se han seguido los siguientes documentos del estándar GSM:

- GSM 03.03 - Numbering, addressing and identification [16].
- GSM 03.07 - Restoration procedures [17].
- GSM 03.08 - Organization of subscriber data [18].
- GSM 03.12 - Location registration procedures [19].
- GSM 03.20 - Security related network functions [20].
- GSM 03.22 - Functions related to Mobile Station (MS) in idle mode and group receive mode [21].
- GSM 04.08 - Mobile Radio Interface [2].
- GSM 05.01 - Physical layer on the radio path; General Description [22].
- GSM 05.02 – Bursts [23].
- GSM 05.03 - Channel coding [24].
- GSM 05.04 - Modulation [13].
- GSM 09.02 - Mobile Application Part (MAP) specification [25].

6.1 Procedimiento attach GSM

El procedimiento de attach en GSM sigue los siguientes pasos [1]:

1. El móvil envía un mensaje de Channel Request al BSS por el canal RACH.
2. El BSS responde con un mensaje de Immediate Assignment por el canal AGCH y asigna un SDCCH al móvil.
3. El móvil envía un Location Update Request por el SDCCH asignado. El móvil envía en ese mensaje el IMSI o el TMSI.
4. El BSS envía un mensaje de Acknowledge al móvil.
5. El BSS envía el Location Update Request al MSC/VLR.
6. El MSC/VLR envía el IMSI al HLR y pide una verificación del IMSI y los "Authentication Triplets" (RAND + SRES + Kc).
7. El HLR envía el IMSI al AuC y pide los "Authentication Triplets".
8. El AuC genera los Authenticacion Triplets y los envía junto al IMSI al HLR.
9. El HLR valida el IMSI y envía el IMSI y los Authenticacion Triplets al MSC/VLR.
10. El MSC/VLR se guarda el SRES y la clave Kc y envía el RAND al BSS y ordena al BSS autenticar al móvil.
11. El BSS envía al móvil un mensaje de Authentication Request. El único parámetro que se envía es el RAND.
12. El móvil usa el RAND para calcular el SRES y envía el SRES al BSS por el SDCCH en un mensaje Authentication Response. El BSS envía el SRES al MSC/VLR.
13. El MSC/VLR compara el SRES recibido con el que tenía guardado y si coinciden la autenticación está completada.
14. El MSC/VLR envía la Kc al BSS y éste se la guarda. El BSS envía el comando Set Cipher Mode al móvil. El mensaje sólo le dice al móvil qué encriptación usar (A5/X).
15. El móvil conmuta al modo cifrado. Envía un mensaje Ciphering Mode Complete al BSS.
16. El MSC/VLR envía un mensaje Location Updating Accept al BSS. También genera un nuevo TMSI para el móvil. El BSS envia el TMSI en un mensaje de TMSI Reallocation Command.
17. El móvil envía un mensaje TMSI Reallocation Complete message al MSC/VLR.
18. El BSS intruye al móvil para ir al modo IDLE enviando un mensaje Channel Release. El BSS elimina el SDCCH.

19. El MSC/VLR envía un mensaje de Update Location al HLR. El HLR guarda en cual MSC/VLR se encuentra el móvil.

Como se puede apreciar, el proceso es bastante largo y complejo, por lo que, como se ha comentado anteriormente, este trabajo se centra, exclusivamente, en los mensajes de la interfaz radio entre el móvil y el BSS. Además, el acknowledge que envía la estación base mientras intercambia mensajes con el MSC no es necesario tampoco. Por tanto, los pasos que se realizan en el trabajo son: 1, 2, 3, 11, 12, 14, 15, 16, 17 y 18.

El diagrama de intercambio de mensajes queda de la siguiente forma:

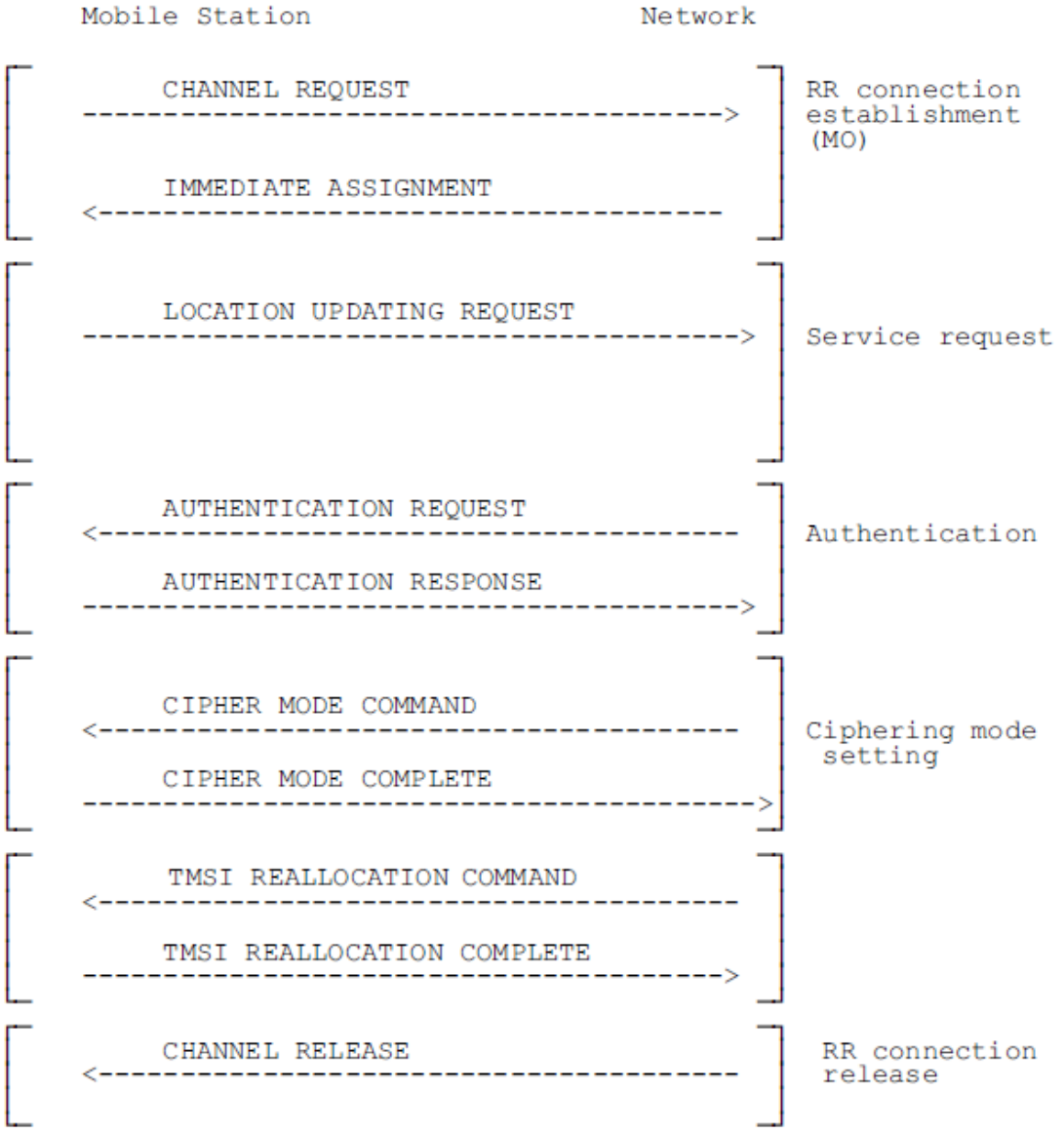


Figura 42: Intercambio de mensajes [2]

5.1 Canal RACH

Como se ha explicado anteriormente, el RACH es un canal común de control por el que se cursan peticiones no programadas, en este caso, una petición de canal para realizar el attach.

5.1.1 Codificación

Por el canal RACH se transmiten 8 bits de información útil que están codificados de la siguiente manera [24]:

1. **Bits de paridad**

Los 8 bits de información van protegidos por 6 bits de paridad que se obtienen de la siguiente forma:

Cuando dividimos $d(0)D^{13} + \cdots + d(7)D^6 + p(0)D^5 + \cdots + p(5)$ entre $D^6 + D^5 + D^4 + D^3 + D^2 + D + 1$ da un resultado igual a $D^6 + D^5 + D^4 + D^3 + D^2 + D + 1$.

A los bits de paridad obtenidos hay que añadirles en módulo 2 el BSIC de la estación base a la que está intentando conectarse el móvil. Con esto se consiguen los 6 bits que finalmente se añaden al mensaje original.

2. **Bits de cola**

Una vez que son añadidos los bits de paridad, hay que añadir 4 bits de cola que están puestos a 0.

3. **Codificador convolucional**

Tras añadir los bits de paridad y de cola al mensaje, todos los bits pasan por un codificador convolucional de tasa ½ definido por los polinomios:

$$G0 = 1 + D^3 + D^4$$

$$G1 = 1 + D + D^3 + D^4$$

Ecuación 9: Polinomios generadores del codificador convolucional

Los bits (e(k) con k desde 0 a 35) se definen según:

$$e(2k) = u(k) + u(k-3) + u(k-4)$$

$$e(2k+1) = u(k) + u(k-1) + u(k-3) + u(k-4)$$

Ecuación 10: Bits de salida

Con k variando desde 0 a 17 y u(k) = 0 para k < 0.

Todo este proceso se realiza en el módulo RACH.vi

RACH.VI

El código LabVIEW de este vi es el siguiente:

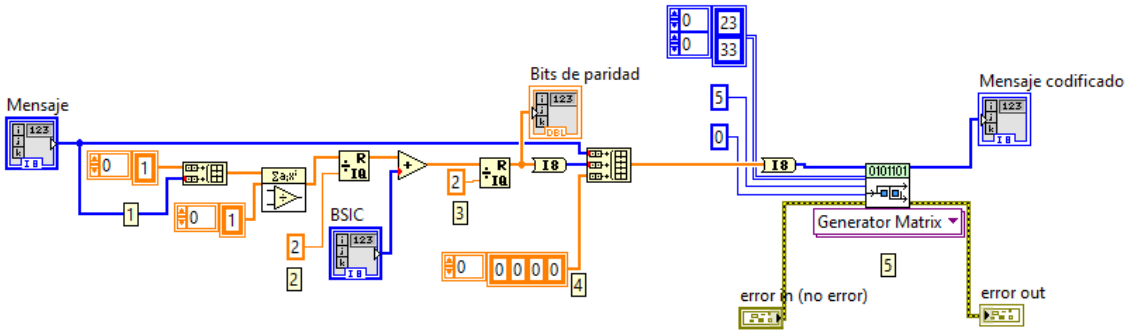


Figura 43: RACH.vi

En este módulo se realiza el anterior proceso de la siguiente manera:

1. Recibe los 8 bits de información que se desean codificar.
2. Se ponen inicialmente los bits de paridad a 1 por lo que al realizar la división con el polinomio convolucional, el resto de esa división son directamente los bits de paridad originales.
3. Para calcular los bits de paridad definitivos, hay que realizar una XOR con el BSIC de la estación base.
4. Se añaden esos bits de paridad y los cuatro bits de cola a 0.
5. Se realiza la codificación convolucional.

Decodificador RACH.VI

El código LabVIEW de este vi es el siguiente:

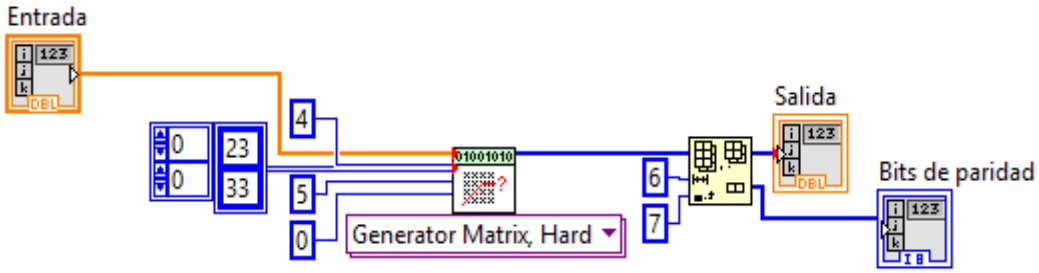


Figura 44: Decodificador RACH.vi

En este módulo se trata de decodificar el canal RACH. Para ello, con los bits recibidos una vez eliminada la ráfaga, se decodifica convolucionalmente de la misma forma que el codificador. El resultado es el mensaje más los bits de paridad, los cuales se eliminan para recuperar el mensaje enviado.

5.2 Canal AGCH y SDCCH

5.2.1 Codificación

La codificación de estos canales se realiza de la siguiente forma [24]:

1. **Código bloque**
    a. Bits de paridad

Los 184 bits de información van protegidos con un código de 40 bits para detectar y corregir errores. Este código se añade a los bits de información de acuerdo con un código FIRE con el siguiente polinomio generador:

$$g(D) = (D^{23} + 1) * (D^{17} + D^3 + 1)$$

Ecuación 11: Polinomio generador del código FIRE

El código FIRE es sistemático y el polinomio que se genera es el siguiente:

$$d(0)D^{223} + d(1)D^{222} + \cdots + d(183)D^{40} + p(1)D^{38} + \cdots + p(38)D + p(39)$$

Ecuación 12: Polinomio generado por el código FIRE

Donde {p(0), p(1), …, p(39)} son los bits de paridad, que, al ser divididos por g(D) dan como resultado: $1 + D + D^2 + \cdots + D^{39}$

    b. Bits de cola

Tras aplicar el código FIRE, se añaden 4 bits a 0 al final de la salida anterior. El resultado es una salida de 228 bits con la siguiente estructura:

$$\begin{cases} u(k) = d(k), & 0 \le k \le 183 \\ u(k) = p(k-148), & 184 \le k \le 223 \\ u(k) = 0, & 224 \le k \le 227 \end{cases}$$

Ecuación 13: Bits de salida del código FIRE más bits de cola

2. **Codificador convolucional**

Tras añadir los bits de paridad y de cola al mensaje, todos los bits pasan por un codificador convolucional de tasa ½ definido por los polinomios:

$$G0 = 1 + D^3 + D^4$$

$$G1 = 1 + D + D^3 + D^4$$

Ecuación 14: Polinomios generadores del codificador convolucional

Los 456 bits codificados (c(k) con k desde 0 a 455) se definen según:

$$c(2k) = u(k) + u(k-3) + u(k-4)$$
$$c(2k+1) = u(k) + u(k-1) + u(k-3) + u(k-4)$$

Ecuación 15: Bits de salida del codificador convolucional

Con k variando desde 0 a 227 y u(k) = 0 para k < 0.

3. Entrelazado

Los bits codificados son entrelazados para evitar errores en bits consecutivos. El entrelazado se realiza según lo siguiente:

$$i(B, j) = c(n, k)$$

Ecuación 16: Fórmula del entrelazado

Donde k, n, B y j varían de la siguiente forma:

$$k = 0, 1, \dots, 227$$
$$n = 0, 1, \dots, N, N+1, \dots$$
$$B = B_0 + 4n + (k \bmod 4)$$
$$j = 2\big((49k) \bmod 57\big) + ((k \bmod 8) \operatorname{div} 4)$$

Ecuación 17: Variación de los valores del entrelazado

Los bits quedan reordenados de la siguiente forma:

k mod 8=	0	1	2	3	k mod 8=	4	5	6	7
j= 0	k = 0	57	114	171	j= 1	228	285	342	399
2	64	121	178	235	3	292	349	406	7
4	128	185	242	299	5	356	413	14	71
6	192	249	306	363	7	420	21	78	135
8	256	313	370	427	9	28	85	142	199
10	320	377	434	35	11	92	149	206	263
	384	441	42	99		156	213	270	327
	448	49	106	163		220	277	334	391
	56	113	170	227		284	341	398	455
	120	177	234	291		348	405	6	63
20	184	241	298	355	21	412	13	70	127
	248	305	362	419		20	77	134	191
	312	369	426	27		84	141	198	255
	376	433	34	91		148	205	262	319
	440	41	98	155		212	269	326	383
30	48	105	162	219	31	276	333	390	447
	112	169	226	283		340	397	454	55
	176	233	290	347		404	5	62	119
	240	297	354	411		12	69	126	183
	304	361	418	19		76	133	190	247
40	368	425	26	83	41	140	197	254	311
	432	33	90	147		204	261	318	375
	40	97	154	211		268	325	382	439
	104	161	218	275		332	389	446	47
	168	225	282	339		396	453	54	111
50	232	289	346	403	51	4	61	118	175
	296	353	410	11		68	125	182	239
	360	417	18	75		132	189	246	303
	424	25	82	139		196	253	310	367
	32	89	146	203		260	317	374	431
60	96	153	210	267	61	324	381	438	39
	160	217	274	331		388	445	46	103
	224	281	338	395		452	53	110	167
	288	345	402	3		60	117	174	231
	352	409	10	67		124	181	238	295
70	416	17	74	131	71	188	245	302	359
	24	81	138	195		252	309	366	423
	88	145	202	259		316	373	430	31
	152	209	266	323		380	437	38	95
	216	273	330	387		444	45	102	159
80	280	337	394	451	81	52	109	166	223
	344	401	2	59		116	173	230	287
	408	9	66	123		180	237	294	351
	16	73	130	187		244	301	358	415
	80	137	194	251		308	365	422	23
90	144	201	258	315	91	372	429	30	87
	208	265	322	379		436	37	94	151
	272	329	386	443		44	101	158	215
	336	393	450	51		108	165	222	279
	400	1	58	115		172	229	286	343
100	8	65	122	179	101	236	293	350	407
	72	129	186	243		300	357	414	15
	136	193	250	307		364	421	22	79
	200	257	314	371		428	29	86	143
	264	321	378	435		36	93	150	207
110	328	385	442	43	111	100	157	214	271
112	392	449	50	107	113	164	221	278	335

Figura 45: Entrelazado [24]

Para estos dos canales se han desarrollado 3 módulos: SDCCH.vi, decodificador SDCCH.vi y entrelazado.vi.

SDCCH.VI

El código LabVIEW de este vi es el siguiente:

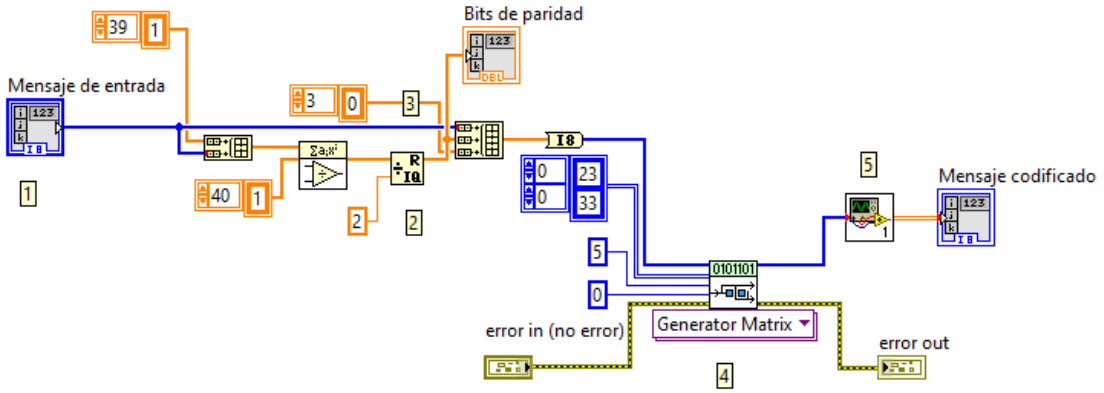


Figura 46: SDCCH.vi

En este módulo se realiza el anterior proceso de la siguiente manera:

1. Recibe los 148 bits de información que se desean codificar.
2. Se ponen inicialmente los bits de paridad a 1 por lo que al realizar la división con el polinomio convolucional, el resto de esa división son directamente los bits de paridad originales.
3. Se añaden los cuatro bits de cola a 0.
4. Se realiza la codificación convolucional.
5. Mediante el módulo entrelazado.vi se entrelazan los bits según la fórmula presentada anteriormente.

Entrelazado.VI

En este módulo hay un bucle for en el que se va realizando el entrelazado. En la primera parte del módulo se realizan los cálculos y en la segunda se van añadiendo los bits a cada uno de los 8 arrays que se utilizan en el entrelazado, uniéndolos, finalmente, en un único array de dos dimensiones.

Decodificador SDCCH.VI

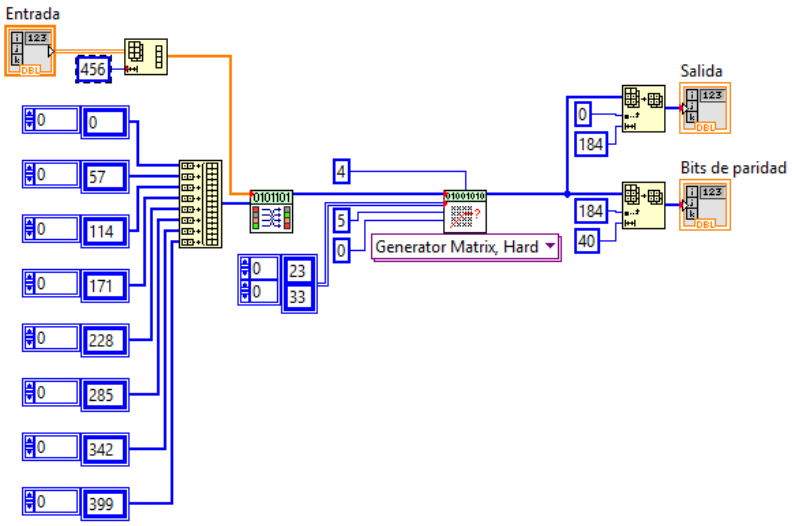


Figura 47: Decodificador SDCCH.vi

En este módulo se realiza la decodificación del canal SDCCH. Para ello, con los mensajes recibidos se crea un array de dos dimensiones del mismo formato que el que sale del codificador que es el que entra como entrada a este vi. Este array de dos dimensiones se aplana y se convierte en un uno de una única dimensión.

Tras obtener este array, usando la una función nativa de LabVIEW llamada MT Permute, se ordenan los bits según indica la tabla de codificación, haciendo que los bits terminen en el orden inicial.

Por último, se realiza de decodificación convolucional, devolviéndose los 184 bits del mensaje original y los 40 bits de paridad que se habían añadido al mensaje.

5.3 Mensajes

5.3.1 Channel Request

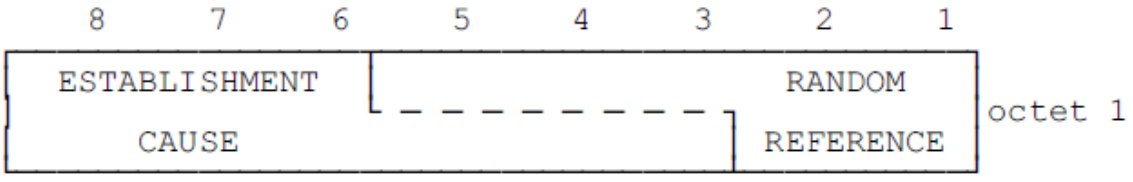


Figura 48: Channel Request [2]

El primer mensaje que envía el móvil es un Channel Request. Este mensaje puede tener muchas opciones de petición según el canal y el procedimiento que se requiera.

En el caso del attach, lo que se necesita es un canal SDCCH, por lo que según indica el estándar GSM, el mensaje debe ser: 0, 0, 0, 1, X, X, X, X.

La formación de este mensaje se realiza en el módulo Channel Request.vi.

5.3.2 Immediate Assignment

Los campos que contiene este mensaje son los siguientes [2]:

Elemento	Presencia	Formato	Longitud (bytes)
L2 Pseudo Length	Obligatoria	V	1
RR management Protocol Dicriminator	Obligatoria	V	1/2
Skip Indicator	Obligatoria	V	1/2
Immediate Assignment Message Type	Obligatoria	V	1
Page Mode	Obligatoria	V	1/2
Spare Half Octet	Obligatoria	V	1/2
Channel Description	Obligatoria	V	3
Request Reference	Obligatoria	V	3
Timing Advance	Obligatoria	V	1
Mobile Allocation	Obligatoria	LV	1-9
Starting Time	Opcional	TV	3
IA Rest Octets (frequency parameters, before time)	Obligatoria	V	0-11

Tabla 1: Immediate Assignment

Este mensaje es el que envía la estación base al móvil para indicar que canal SDCCH debe usar. Este mensaje se envía por el canal AGCH.

La formación de este mensaje se realiza en el módulo Immediate Assignment.vi.

5.3.3 Location Update Request

Los campos que contiene este mensaje son los siguientes [2]:

Elemento	Presencia	Formato	Longitud (bytes)
Mobility management protocol distriminator	Obligatoria	V	1/2
Skip Indicator	Obligatoria	V	1/2
Location Updating Request message type	Obligatoria	V	1
Location updating type	Obligatoria	V	1/2
Ciphering key sequence number	Obligatoria	V	1/2
Location area identification	Obligatoria	V	5
Mobile station classmark	Obligatoria	V	1
Mobile identity	Obligatoria	LV	2-9

Tabla 2: Location Update Request

Este mensaje es enviado por el móvil para realizar la petición del IMSI attach o de location update. En él, el móvil indica su identidad mediante su IMSI o TMSI y su localización. Tambíen, mediante el campo de Location updating type indica que su petición es para realizar el IMSI attach.

Este mensaje ya se envía por el canal SDCCH asignado al usuario.

La formación de este mensaje se realiza en el módulo Location Update.vi.

5.3.4 Authentication Request

Los campos que contiene este mensaje son los siguientes [2]:

Elemento	Presencia	Formato	Longitud (bytes)
Mobility management protocol distriminator	Obligatoria	V	1/2
Skip Indicator	Obligatoria	V	1/2
Authentication Request message type	Obligatoria	V	1
Ciphering key sequence number	Obligatoria	V	1/2
Spare half octect	Obligatoria	V	1/2
Authentication RAND	Obligatoria	V	16

Tabla 3: Authentication Request

Este mensaje sirve para comenzar el proceso de autenticación del móvil. En él la estación base envía el parámetro RAND que recibiría del MSC y que permite al móvil autenticarse.

La formación de este mensaje se realiza en el módulo Authentication Request.vi.

5.3.5 Authentication Response

Los campos que contiene este mensaje son los siguientes [2]:

Elemento	Presencia	Formato	Longitud (bytes)
Mobility management protocol distriminator	Obligatoria	V	1/2
Skip Indicator	Obligatoria	V	1/2
Authentication Response message type	Obligatoria	V	1
Authentication parameter SRES	Obligatoria	V	1/2

Tabla 4: Authentication Response

El Authentication Response sirve para que el móvil envíe el SRES calculado a partir del parámetro RAND enviado por la estación base.

La formación de este mensaje se realiza en el módulo Authentication Response.vi.

5.3.6 Set Cipher Mode

Los campos que contiene este mensaje son los siguientes [2]:

Elemento	Presencia	Formato	Longitud (bytes)
RR management protocol distriminator	Obligatoria	V	1/2
Skip Indicator	Obligatoria	V	1/2
Cipher Mode Command message type	Obligatoria	V	1
Ciphering Mode Setting	Obligatoria	V	1/2
Cipher Response	Obligatoria	V	1/2

Tabla 5: Set Cipher Mode

Una vez completada la autenticación, la estación base envía el mensaje de Set Cipher Mode para comenzar la encriptación de la comunicación. En él se indica qué encriptación usar (A5/X).

La formación de este mensaje se realiza en el módulo Authentication Response.vi.

5.3.7 Cipher Mode Complete

Los campos que contiene este mensaje son los siguientes [2]:

Elemento	Presencia	Formato	Longitud (bytes)
RR management protocol distriminator	Obligatoria	V	1/2
Skip Indicator	Obligatoria	V	1/2
Cipher Mode Complete message type	Obligatoria	V	1
Mobile Equipment Identity	Opcional	TLV	3-11

Tabla 6: Cipher Mode Complete

Este mensaje enviado por el móvil a la estación base únicamente sirve para comunicar que se ha completado el proceso para comenzar a cifrar la conexión.

La formación de este mensaje se realiza en el módulo Cipher Mode Complete.vi.

5.3.8 TMSI Reallocation Command

Los campos que contiene este mensaje son los siguientes [2]:

Elemento	Presencia	Formato	Longitud (bytes)
Mobility management protocol distriminator	Obligatoria	V	1/2
Skip Indicator	Obligatoria	V	1/2
TMSI Reallocation Command message type	Obligatoria	V	1
Location area identification	Obligatoria	V	5
Mobile identity	Obligatoria	LV	2-9

Tabla 7: TMSI Reallocation Command

Una vez está cifrada la conexión entre el móvil y la estación base, ésta envía un mensaje de TMSI Reallocation Command. Este mensaje se utiliza para que la red proporcione al usuario un TMSI para usar.

La formación de este mensaje se realiza en el módulo TMSI Reallocation Command.vi.

5.3.9 TMSI Reallocation Complete

Los campos que contiene este mensaje son los siguientes [2]:

Elemento	Presencia	Formato	Longitud (bytes)
Mobility management protocol distriminator	Obligatoria	V	1/2
Skip Indicator	Obligatoria	V	1/2
TMSI Reallocation Complete message type	Obligatoria	V	1

Tabla 8: TMSI Reallocation Complete

Con este mensaje el móvil indica que el proceso de cambio del TMSI se ha realizado.

La formación de este mensaje se realiza en el módulo TMSI Reallocation Complete.vi.

5.3.10 Channel Release

Los campos que contiene este mensaje son los siguientes [2]:

Elemento	Presencia	Formato	Longitud (bytes)
RR management protocol distriminator	Obligatoria	V	1/2
Skip Indicator	Obligatoria	V	1/2
Channel Release message type	Obligatoria	V	1
RR Cause	Obligatoria	V	1
BA Range	Opcional	TLV	6-?
Group Channel Description	Opcional	TLV	4-13
Group Cipher Key Number	Condicional	TLV	1 1/2

Tabla 9: Channel Release

Por último, el último mensaje que se envía es el de Channel Release. En este mensaje, la BTS le indica al móvil que el canal SDCCH utilizado queda liberado.

La formación de este mensaje se realiza en el módulo Channel Release.vi.

5.4 Inserción en la ráfaga

La inserción de los bits de información dentro de las correspondientes ráfagas se realiza en el módulo Burst modificado.vi, en el que se encuentran las ráfagas Normal Burst, Frequency Correction Burst, Synchronization Burst y Access Burst.

5.4.1 Canal RACH

Como se ha detallado en la parte de explicación del estándar GSM, el canal RACH utiliza una ráfaga tipo Access Burst.

Los campos que contiene esta ráfaga y sus valores reales son:

- **Extended tails bits:** 0, 0, 1, 1, 1, 0, 1, 0.
- **Synchonization sequence bits:** 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0.
- **Encrypted bits:** bits de información codificados que se desean enviar.
- **Tails bits:** 0, 0, 0.

En la siguiente imagen se muestra como se realiza la inserción en LabVIEW:

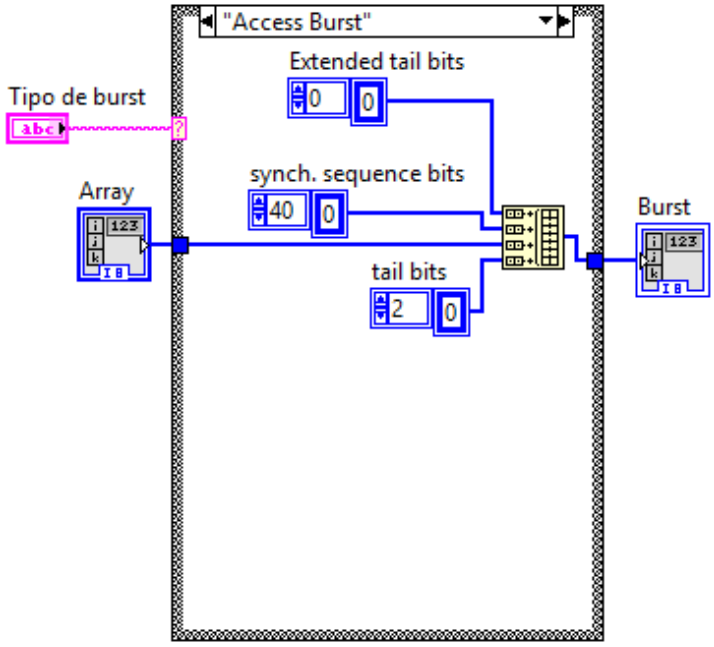


Figura 49: Burst modificado.vi. Access Burst

Primeramente, este módulo recibe como entrada el tipo de ráfaga que se desea y los bits codificados que hay que enviar. En este caso, el tipo de ráfaga será "Access Burst" y el array serán los 36 bits codificados del canal RACH.

Despues, y tal como indica el estándar de GSM, se añaden los campos extended tail bits, synchronization sequence bits y tail bits con los valores anteriores y así resulta la ráfaga a enviar.

5.4.2 Canales SDCCH y AGCH

Los canales SDCCH y AGCH utilizan una ráfaga tipo Normal Burst.

La Normal Burst contiene estos campos:

- ***Tail Bits:*** 0, 0, 0.
- **Encrypted bits:** los 57 primeros bits de información que se desean enviar.
- **Training Sequence Bits:** puede tener 7 valores. En el caso de estos canales de control, la secuencia se elige según el BCC.
    - TS0: 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1.
    - TS1: 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1.
    - TS2: 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0.
    - TS3: 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0.
    - TS4: 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1.
    - TS5: 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0.
    - TS6: 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1.
    - TS7: 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0.
- **Encrypted bits:** los siguientes 57 bits de información.
- **Tail Bits:** 0, 0, 0.

La siguiente figura muestra el proceso en LabVIEW:

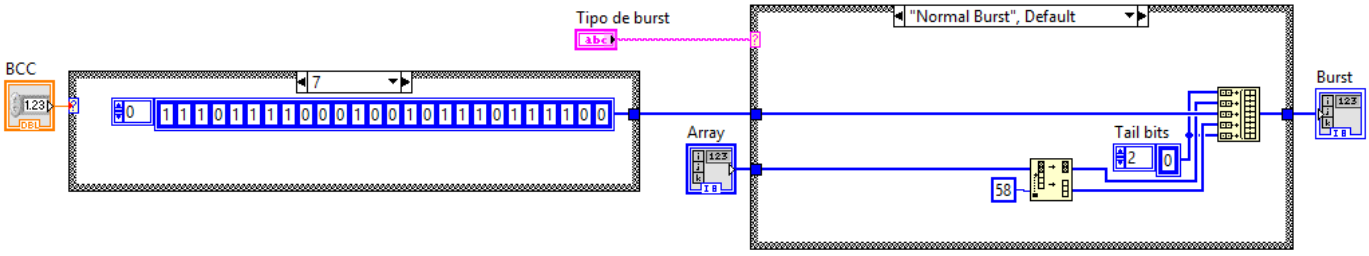


Figura 50: Burst modificado.vi. Normal Burst

Este vi tiene como entradas el tipo de ráfaga, el mensaje a enviar (114 bits) y el BCC.

Con el BCC se elige la secuencia de entrenamiento que se debe incluir en la ráfaga y, después, se añaden todos los campos necesarios para formar la ráfaga.

5.5 Transmisión

Una vez que están los mensajes insertados en la ráfaga hay que continuar con el proceso de transmisión de GSM. .

En este trabajo lo primero que se realiza es la modulación del mensaje insertado en la ráfaga. Tras la modulación, hay que formar el slot añadiendo el periodo de guarda de cada canal y, finalmente, se forma la trama añadiendo otros 7 slots, que, en este caso, estarán vacíos.

5.5.1 Modulador

La modulación se realiza tal y como se explicó en el apartado 2.5.7 de este trabajo.

El módulo encargado de la modulación es Modulador.vi y su código se muestra en la siguiente figura:

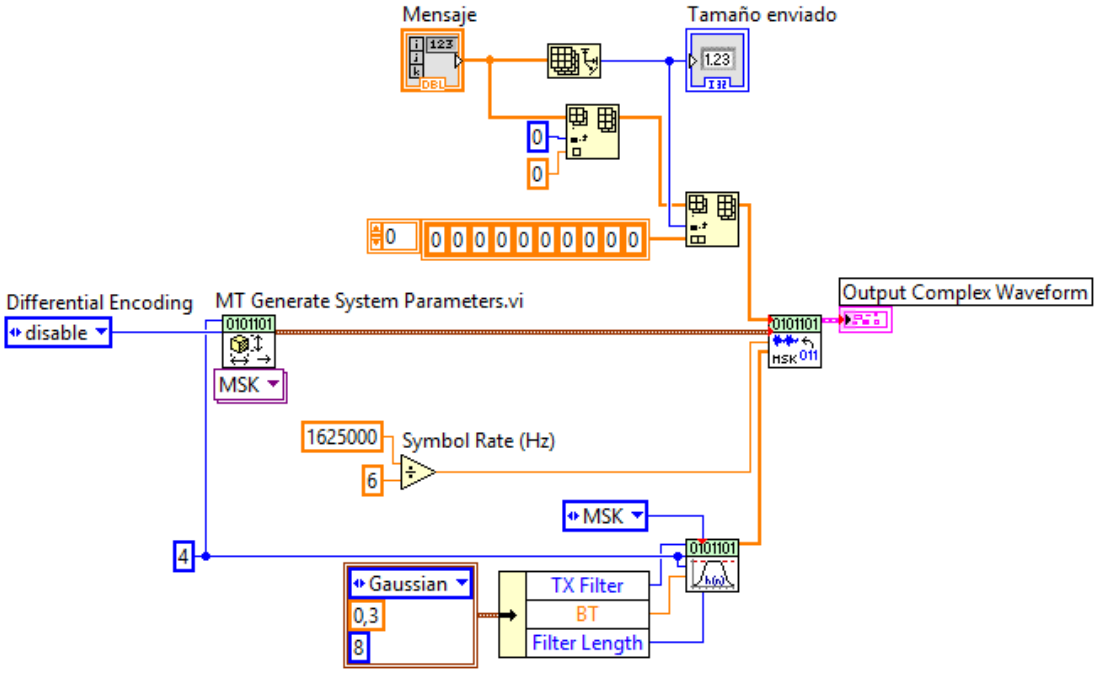


Figura 51: Modulador.vi

En este módulo se utilizan tres módulos proporcionados por National Instrumets en el paquete Modulation Toolkit: MT Generate System Parameters VI, MT Generate Filter Coefficients y MT Modulate MSK.

Con el primer módulo, únicamente genera unos parámetros de configuración para posteriormente utilizarlos en el modulador. Recibe como entrada si se desea o no codificación diferencial (desactivada al no ser la misma que en GSM) y el número de muestras por símbolo que en este caso son cuatro.

El segundo módulo tiene como salida los coeficientes del filtro que se quiera en la modulación. Como entrada tiene los parámetros necesarios para generar los coeficientes:

- **Tipo de modulación:** MSK.
- **Número de muestras por símbolo:** 4.
- **Tipo de filtro:** Gaussiano.
- **BT:** 0,3.
- **Longitud del filtro:** 8 símbolos.

Por último, el modulador recibe las salidas de los dos módulos anteriores, la tasa de símbolo (270833,33 Hz) y el mensaje que se desea modular y devuelve la forma de onda como salida.

5.5.2 Formación del slot

La formación del slot se realiza como se explicó en el apartado 2.5.2, donde se detallan los tipos de ráfagas y sus campos.

Esta formación del slot se realiza en el módulo CreateSlots.vi. En él se reciben parámetros como el tipo de ráfaga, el mensaje que se desea modular y otros datos que se necesitan para formar algunas ráfagas.

El código LabVIEW de la formación del slot se muestra en las figuras 53 (Normal Burst) y 54 (ráfaga vacía) y 55 (Access Burst).

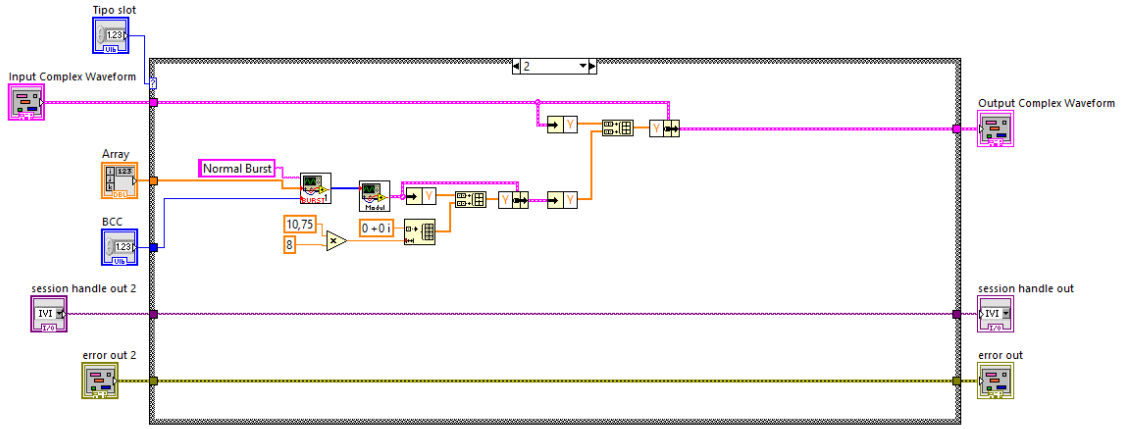


Figura 52: CreateSlots.vi. Normal Burst

En el caso de la Normal Burst, se utiliza, además de los parámetros normales, el BCC, para seleccionar la secuencia de entrenamiento que debe llevar la ráfaga. Se utilizan otros módulos explicados anteriormente como Burst.vi y Modulador.vi.

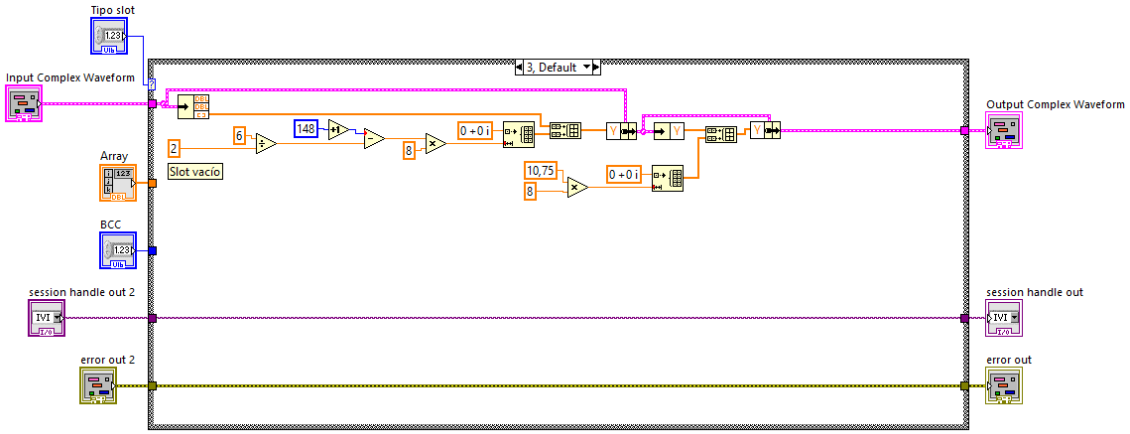


Figura 53: CreateSlots.vi. Ráfaga vacía

Cuando no hay datos que enviar se crea un slot vacío. En este caso lo único que hay que hacer es una forma de onda en la que todos los valores sean nulos (0 + 0i) para no enviar ningún tipo de información.

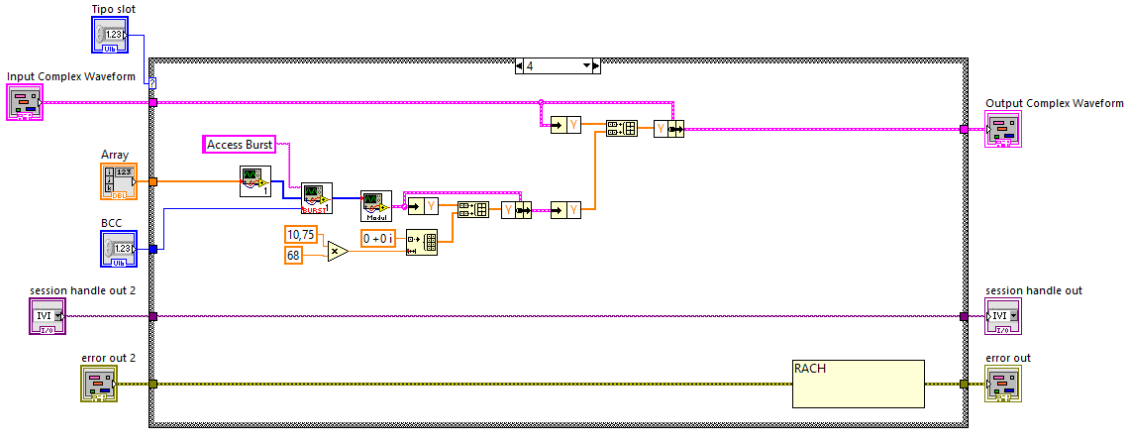


Figura 54: CreateSlots.vi. Access Burst

Con la ráfaga de acceso utilizada en el RACH, el funcionamiento es similar a la Normal Burst, se recibe el mensaje que, posteriormente, se inserta en la ráfaga Access Burst y después se modula y se le añade el tiempo de guarda.

5.5.3 Formación de la trama

Para la formación de la trama completa únicamente hay que reunir 8 slots con sus correspondientes tiempos de guarda.

Esta formación de la trama se realiza en el módulo Slots.vi y su código LabVIEW es el siguiente:

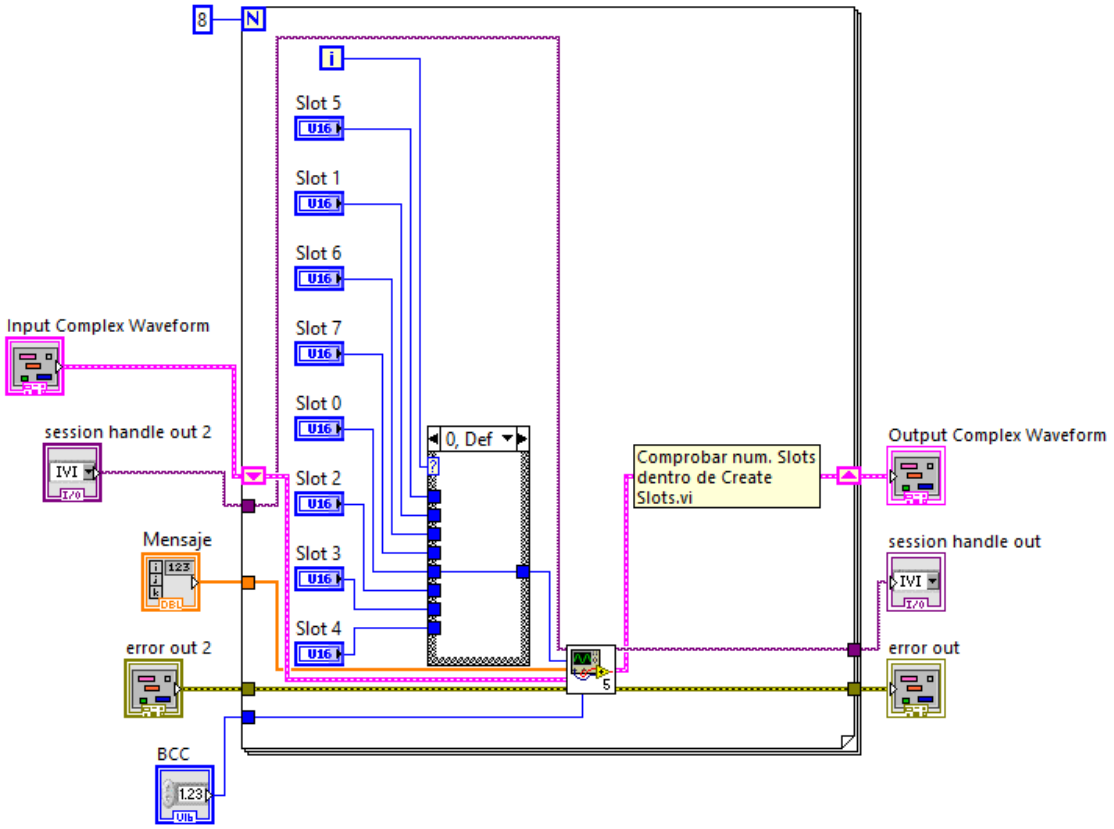


Figura 55: Slots.vi

Para la formación de la ráfaga, se crea un bucle for de 8 interacciones en el que, mediante el módulo CreateSlots.vi se van creando los 8 slots y se unen.

5.6 Recepción

Como se ha explicado anteriormente, la sincronización no se realiza de la misma forma que se detalla en el estándar de GSM. En este caso, el receptor, tanto de la estación base como del móvil, detecta patrones predefinidos como son la secuencia de entrenamiento en mensajes enviados con la Normal Burst y los bits de sincronización en el caso de mensajes enviados con la Access Burst.

Una vez detectados esos patrones, el mensaje recibido se compara con el mensaje esperado. Si el mensaje recibido es igual al esperado, se da por bueno y se continúa con la recepción del siguiente mensaje. En caso contrario, la recepción permanece recibiendo el mismo mensaje.

La recepción de los mensajes se realiza mediante el módulo Receptor Patrón.vi

5.6.1 Receptor Patrón.vi

En este VI se realiza tanto la recepción como la demodulación de los mensajes su código LabVIEW es el siguiente:

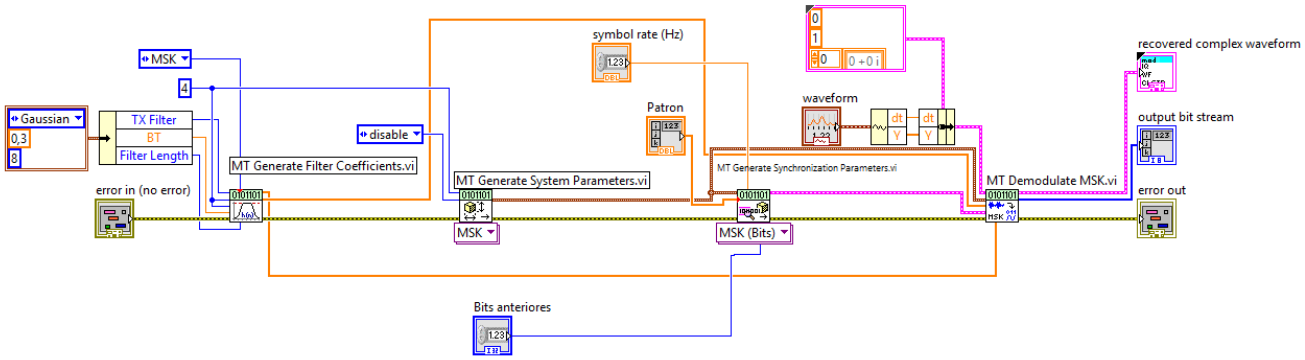


Figura 56: Receptor Patrón.vi

En este vi se utilizan cuatro módulos proporcionados por National Instrumets en el paquete Modulation Toolkit: MT Generate Filter Coefficients, MT Generate System Parameters, Generate Synchronization Parameters y MT Demodulate MSK.

Con el primer vi se generan los coeficientes del filtro necesarios para la modulación GMSK de GSM. Para ello recibe algunos parámetros:

- **Tipo de modulación:** MSK.
- **Número de muestras por símbolo:** 4.
- **Tipo de filtro:** Gaussiano.
- **BT:** 0,3.
- **Longitud del filtro:** 8 símbolos.

En el segundo vi simplemente se generan parámetros de configuración necesarios para la demodulación del mensaje. Para ello recibe dos parámetros que son el número de muestras por símbolo (4) y si se desea codificación diferencial. En este caso, al igual que en el modulador, la codificación diferencial está desactivada.

El vi Generate Synchronization Parameters es de gran importancia en este trabajo debido a la falta de implementación de la sincronización del estándar GSM. Este vi permite realizar la recepción de mensajes mediante un patrón conocido. Recibe, además de los parámetros de configuración anteriores, los siguientes datos de entrada:

- **Sync bits:** estos bits de sincronización se refieren al patrón conocido del mensaje que se desea recibir. En este caso, como se ha explicado

anteriormente, serán las secuencias de entrenamiento de la Normal Burst o los bits de sincronización de la ráfaga Access Burst.

- **Sync indent:** esta entrada indica el número de símbolos previos al patrón anterior. En el caso de la Normal Burst serán 61 mientras que, en el caso de la Access Burst serán 8.

Por último, el MT Demodulate MSK es el vi que se encarga de la demodulación propiamente dicha y devuelve lo bits demodulados. Recibe las salidas de los vi anteriores (coeficientes del filtro, parámetros de configuración y parámetros de sincronización) y, también, la forma de onda recibida.

5.7 Otras funciones

5.7.1 Elegir Mensaje Modulado

Con el módulo Elegir Mensaje Modulado.vi simplemente el emisor elige que mensaje enviar. Para ello, en el caso del RACH simplemente se modula el mensaje y se inserta en la trama y, en el caso del AGCH y SDCCH, se modula y se inserta en cuatro tramas consecutivas.

5.7.2 Comparador

Para comparar la secuencia recibida con los bits esperados se crea un módulo llamado comparador.vi cuyo código es el siguiente:

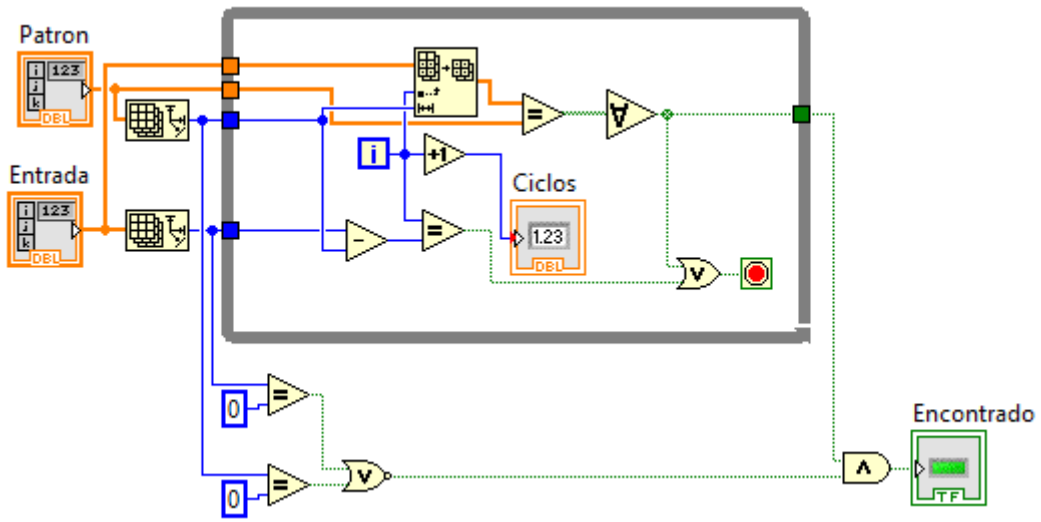


Figura 57: Comparador.vi

Este módulo recibe como entrada el mensaje completo y el patrón con el que se desea comparar. Después hay un bucle for que va recorriendo todo el mensaje y va

comparando cada parte con el patrón original. Este bucle for para cuando se encuentra o cuando se ha recorrido todo el mensaje sin encontrar el patrón. Como salida tiene un boolean que indica si se ha encontrado ese patrón en el mensaje o no.

5.8 Interfaz de usuario

Todos estos elementos se reúnen en dos interfaces de usuarios para cumplir la funcionalidad completa.

5.8.1 Configuración del emisor

La configuración del emisor en la BTS y en el móvil se realiza de la siguiente manera:

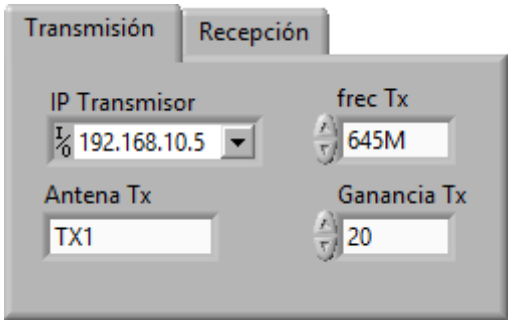


Figura 58: Configuración emisor BTS

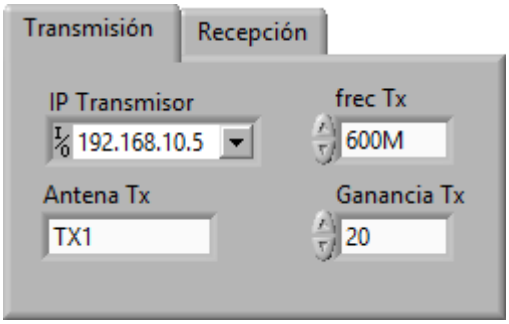


Figura 59: Configuración emisor móvil

Para usar bandas de frecuencia poco utilizadas y que no produzcan interferencias se usa la banda de 600 MHz. Además, tal y como se indica en el estándar GSM, la frecuencia del enlace de bajada está 45 MHz por encima de la frecuencia del canal de subida.

Por otra parte, ambos transceptores utilizaran como antena de transmisión la TX1 con una ganancia de 20 dB.

El código LabVIEW que se ejecuta para la configuración de la transmisión es el siguiente:

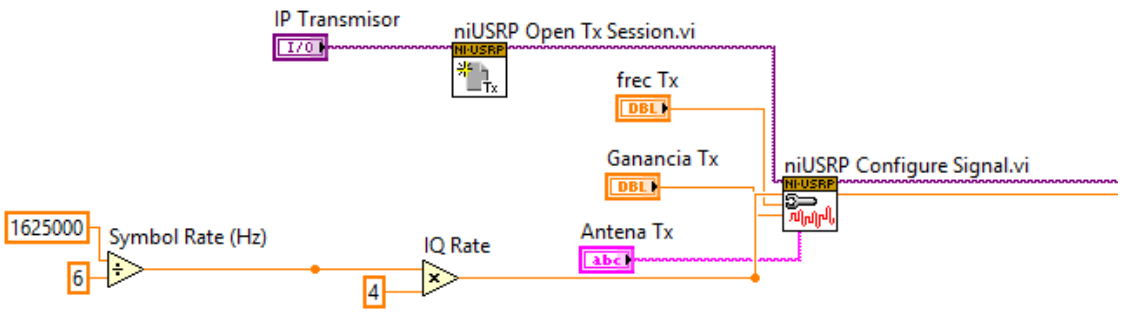


Figura 60: Configuración de la transmisión

Como se ve en la anterior imagen, lo primero que se hace es abrir una sesión con el transceptor USRP. Tras eso, se configura la señal con los parámetros anteriores y el IQ rate teórico.

5.8.2 Configuración del receptor

La configuración del receptor se realiza de forma similar a la del transmisor:

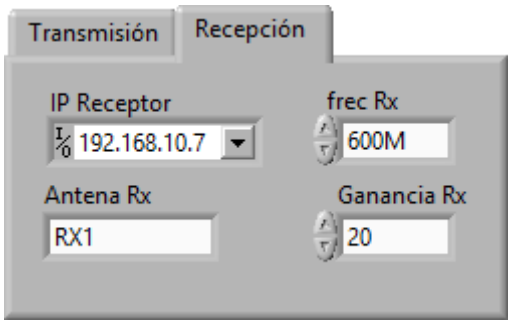


Figura 61: Configuración receptor BTS

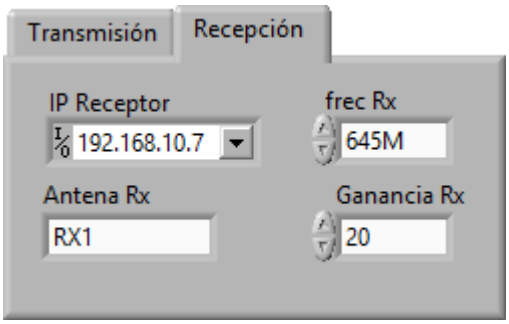


Figura 62: Configuración receptor móvil

Sin embargo, el código LabVIEW de la configuración es distinto:

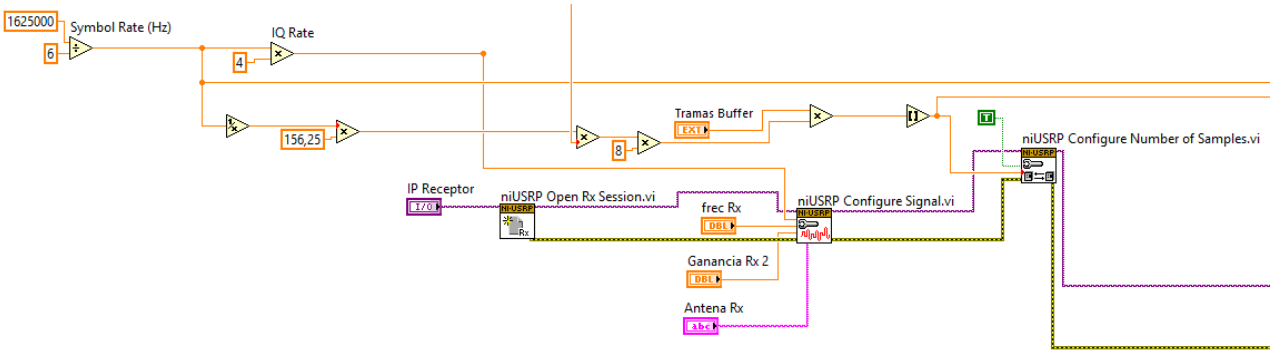


Figura 63: Configuración de la recepción

En este caso, además de abrir la sesión con el USRP y configurar la señal con los parámetros necesarios, hay que configurar el número de muestras que queremos obtener. Para ello, en la interfaz de usuario hay un parámetro configurable llamado "Tramas Buffer" en el que podemos decidir cuantas tramas GSM queremos obtener en cada recepción.

5.8.3 Transmisión

La transmisión se realiza de forma similar tanto en el móvil como en la BTS. El código LabVIEW se basa en un bucle while, que va enviando el mensaje modulado (recibido del vi "Elegir mensaje modulado") hasta que recibe la primera parte del mensaje siguiente, dentro de un bucle for que es el que va cambiando de estado.

El código necesario para la transmisión es el siguiente:

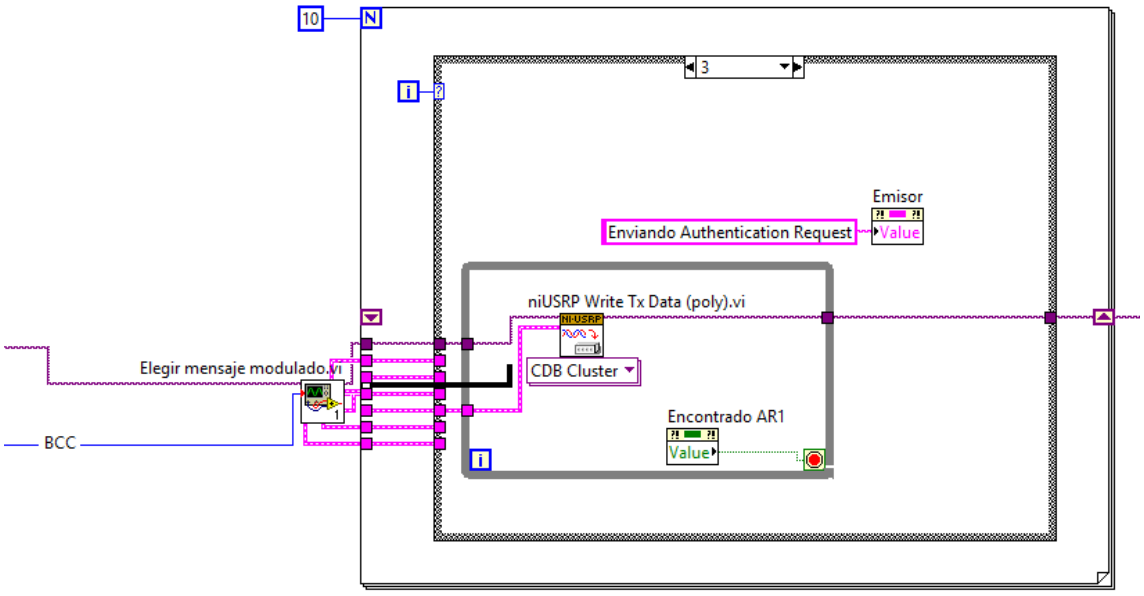


Figura 64: Ejemplo de transmisión en BTS

5.8.4 Recepción

El proceso de recepción es similar al de transmisión. El en caso de la recepción del Channel Request enviado en el RACH, la recepción se realiza en un bucle while en el que se intenta recibir el mensaje con los bits de sincronización de la ráfaga y, después, se compara con el mensaje esperado. Tras comprobar que es el mensaje correcto, el bucle for que lo engloba pasa al siguiente estado.

Para recibir el AGCH y el SDCCH el proceso es similar, únicamente cambia que, en lugar de un único bucle while en cada estado, hay cuatro, debido a que los mensajes de estos canales se reparten en cuatro tramas distintas.

5.8.5 Parámetros configurables

En la interfaz de usuario hay dos parámetros configurables: tramas buffer y BSIC tal y como muestra la siguiente figura:

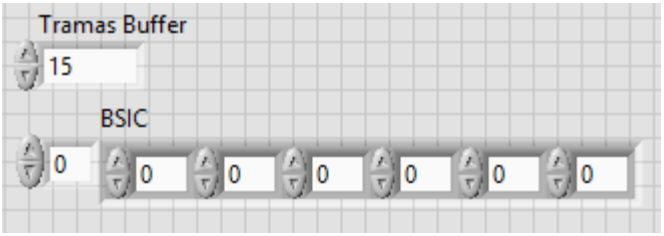


Figura 65. Parámetros configurables

- **Tramas Buffer:** este número indica el número de tramas GSM que se desean obtener en cada recepción. Encontrar el valor correcto es complicado debido a que, si el número es alto, la recepción será más lenta pero la probabilidad de encontrar el mensaje es mayor, por el contrario, si el número es bajo, la recepción es más rápida pero la probabilidad de encontrar el mensaje es mejor. En las pruebas se han usado los valores 8 y 15.
- **BSIC:** es el número que identifica a la estación base. Este número se utiliza en la codificación del RACH. Además, los tres últimos bits del BSIC, el BCC, se utiliza para elegir la secuencia de entrenamiento de la Normal Burst.

5.8.6 Estado del transmisor y receptor

En la interfaz de usuario se muestra lo que está realizando el receptor y el emisor, tanto de la estación base como del móvil:

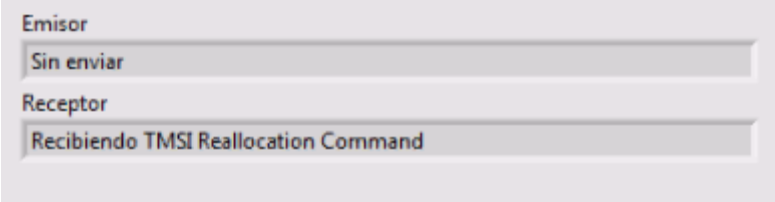


Figura 66. Ejemplo de estado

5.8.7 Mensaje recibido y decodificado

En la interfaz también se muestran los mensajes que se van recibiendo antes y después de su codificación:

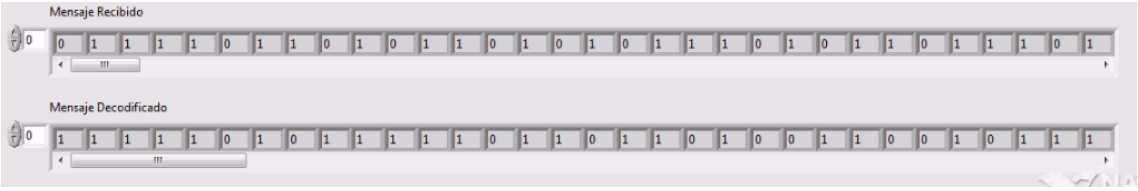


Figura 67. Ejemplo de mensaje recibido y decodificado.

5.8.8 Estado del procedimiento attach

La parte más importante de la interfaz de usuario es la que indica en qué estado del procedimiento attach se encuentra el programa. Para ello, hay una serie de leds que indican que mensajes se van recibiendo:

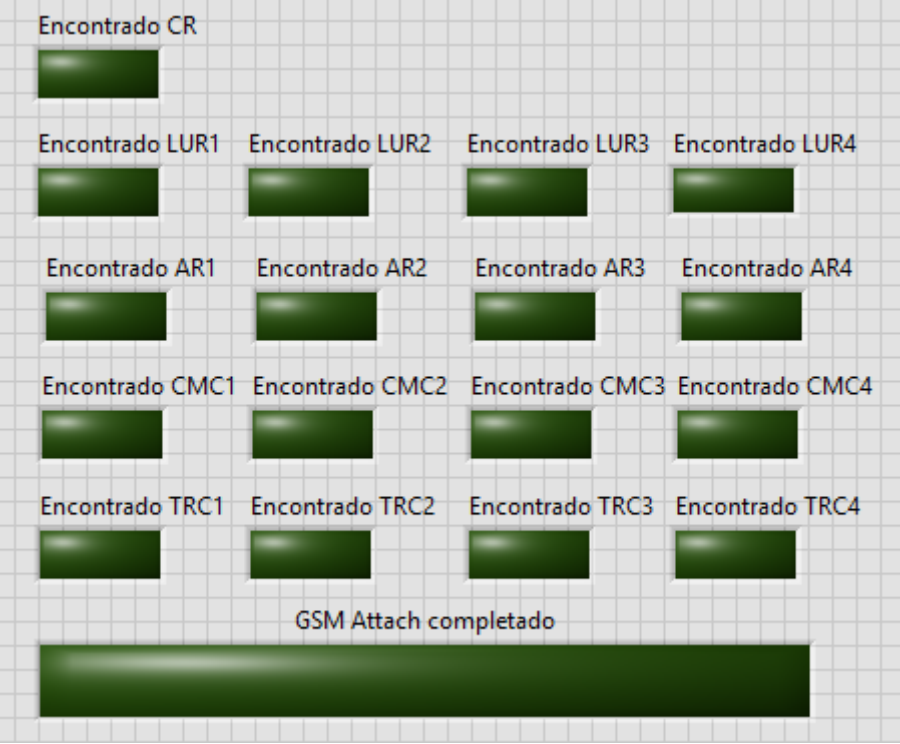


Figura 68: Estado del procedimiento attach en BTS

Figura 69: Estado del procedimiento attach en estación móvil

5.8.9 Interfaz de usuario final

Finalmente, tras unir todos los elementos, las interfaces que manejara el usuario, tanto del móvil como de la BTS serán las siguientes:

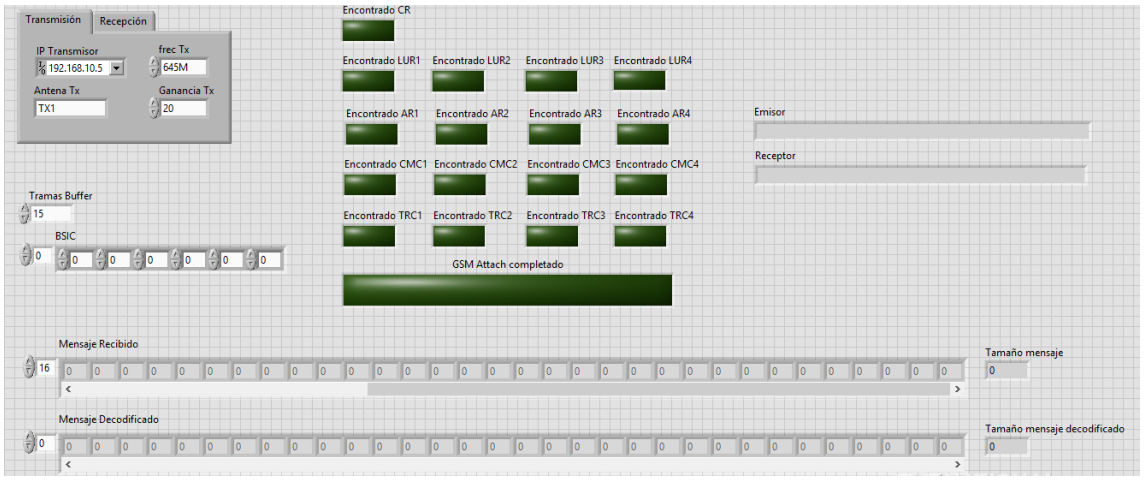


Figura 70: Interfaz final de BTS

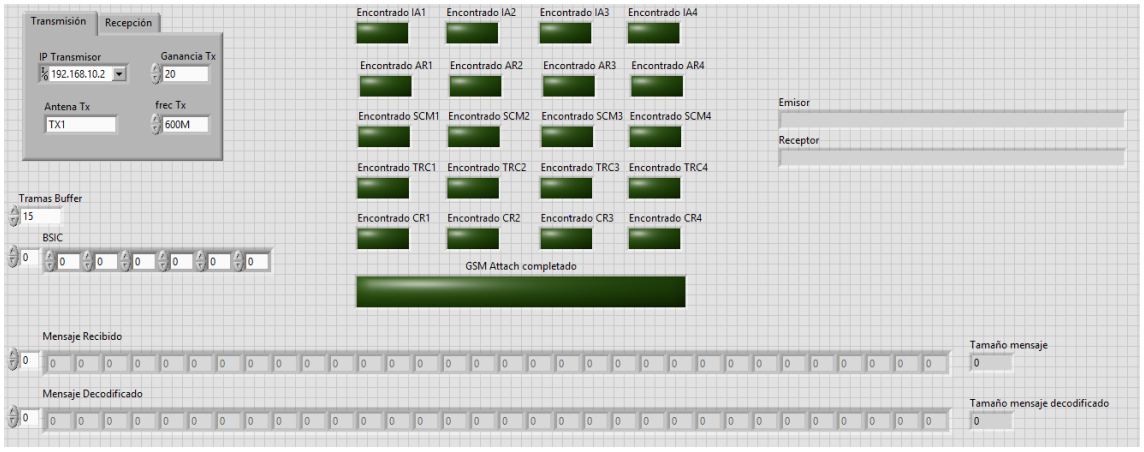


Figura 71. Interfaz final de la estación móvil

6 Pruebas y resultados

Las pruebas de este trabajo se han estado realizando tanto durante su desarrollo como después de terminarlo. Además, se han intentado ejecutar las máximas pruebas posibles y a todos los módulos.

6.1 Codificación y decodificación

Las primeras pruebas se realizaron a los módulos que codifican y decodifican la información. Para ello simplemente se juntan los módulos que codifican y los que decodifican para ver si se obtiene el mismo resultado. Los resultados de esta prueba fueron los esperados y todo funcionaba correctamente.

6.2 Modulación

Otra de las pruebas más importantes y que permitió descubrir errores fue las que se realizaron a los módulos de la modulación y demodulación.

Para ello, se creó el siguiente vi:

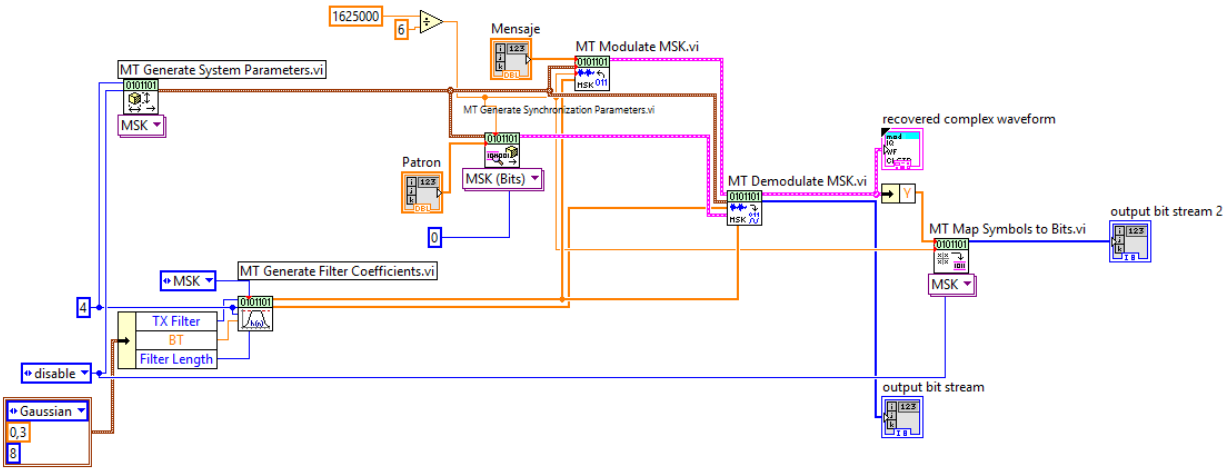


Figura 72: Prueba modulación-demodulación.vi

Con este vi se comprobó que la modulación no funcionaba como se esperaba.

Por una parte, la codificación diferencial no tenía los mismos resultados que los que tiene GSM, por lo que se decidió desactivarla.

Por otra, tras modular los bits y demodularlos posteriormente, los bits recuperados no eran los previstos. El mensaje demodulado estaba incompleto, ya que, al principio de éste faltaba un bit y al final faltaban 10. Gracias a esta prueba se pudo completar el modulador, añadiendo el código LabVIEW necesario para que los bits puedan llegar completos. Este código es el siguiente:

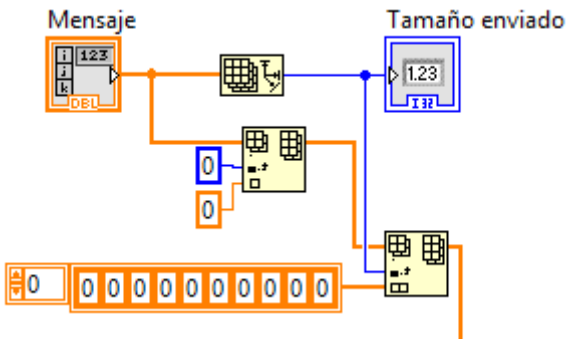


Figura 73: Código añadido a modulador.vi

6.3 Transmisión

La transmisión es una de las partes que más problemas ha dado y, por tanto, las pruebas han sido varias.

Durante la primera fase del desarrollo, para comprobar que la transmisión se realizaba en la frecuencia correcta se utilizaba el analizador vectorial de señales, donde indica el espectro.

El espectro obtenido se muestra en las figuras 75 (600 MHz) y 76 (645 MHz).

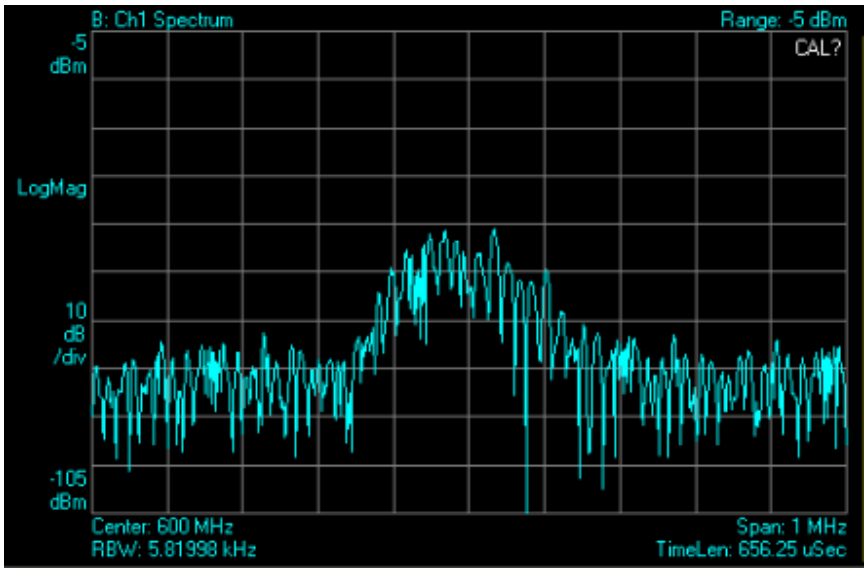


Figura 74: Espectro 600 MHz

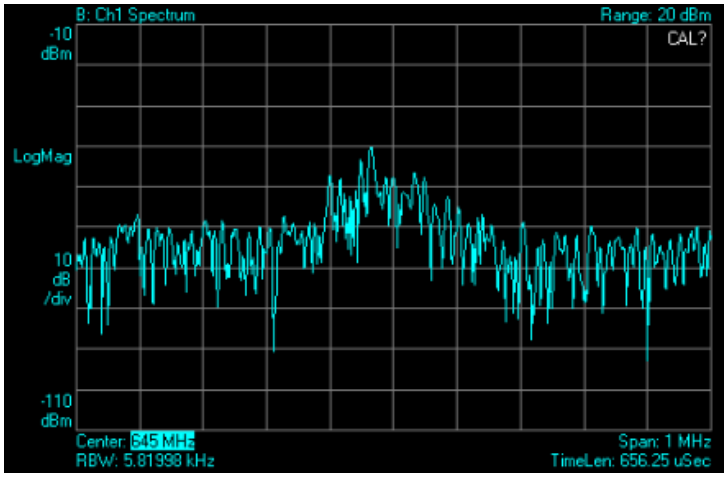


Figura 75: Espectro 645 MHz

Una vez comprobado que la transmisión se efectuaba en las frecuencias correctas, se prueba el programa final para ver si el funcionamiento correcto tal y como se muestra en las siguientes imágenes:

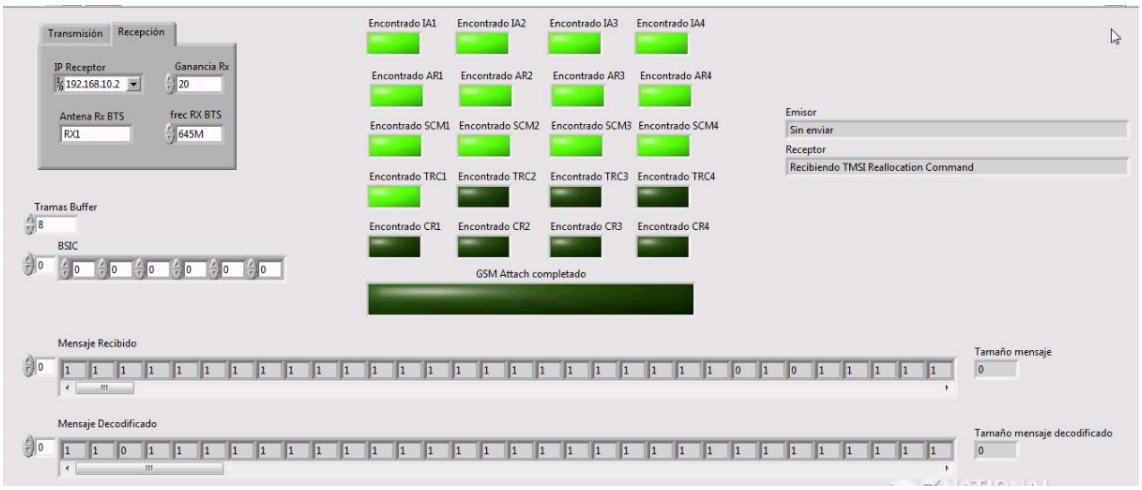


Figura 76: Funcionamiento correcto del móvil

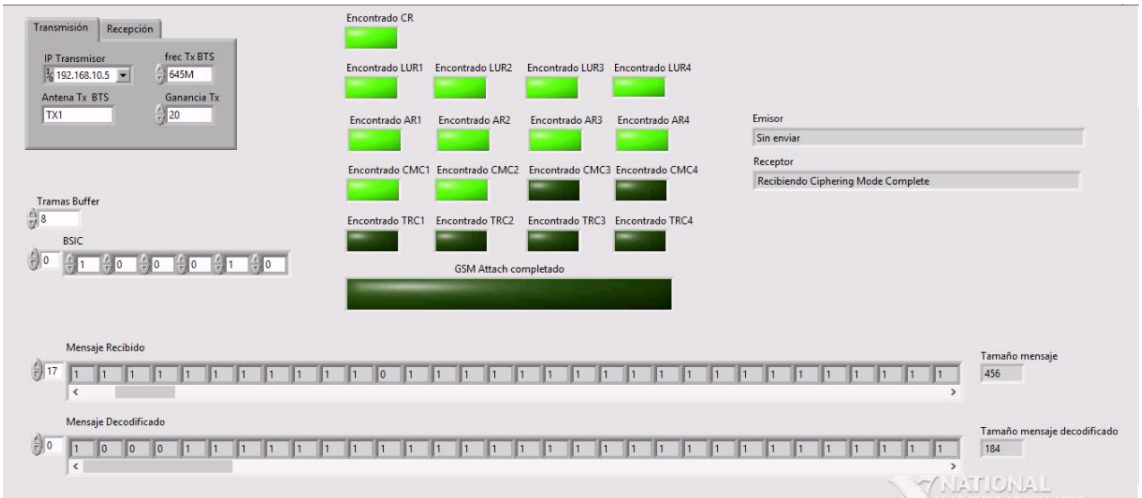


Figura 77: Funcionamiento correcto de BTS

Tal y como se aprecia en las anteriores imágenes, el programa funciona correctamente, recibiendo y enviando los mensajes esperados.

Visto el correcto funcionamiento del programa, se realizaron distintas capturas con el analizador vectorial de señales para comprobar el funcionamiento.

Canal RACH:

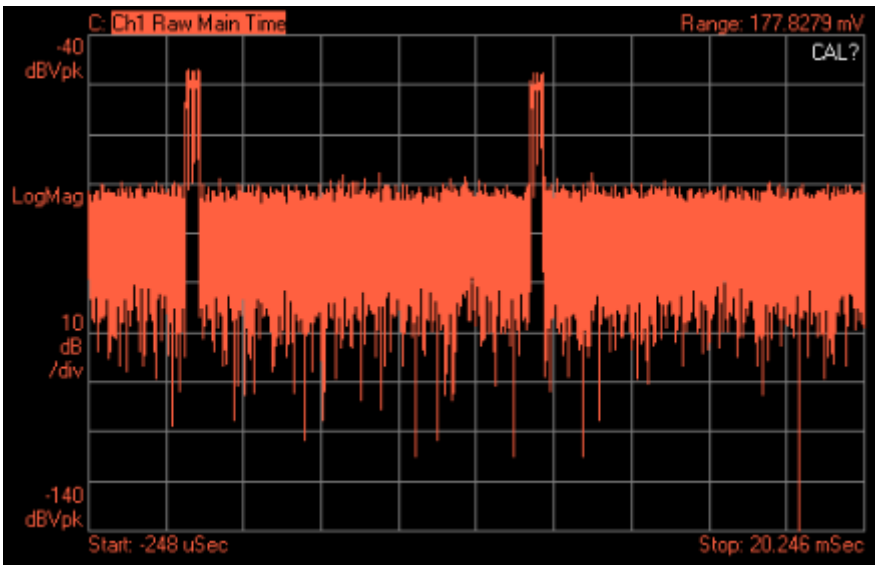


Figura 78. Transmisión del RACH

En esta captura se puede ver que el funcionamiento es el correcto. La mayor parte del tiempo no hay transmisión mientras que, en cortos periodos de tiempo se produce la transmisión.

Canal AGCH:

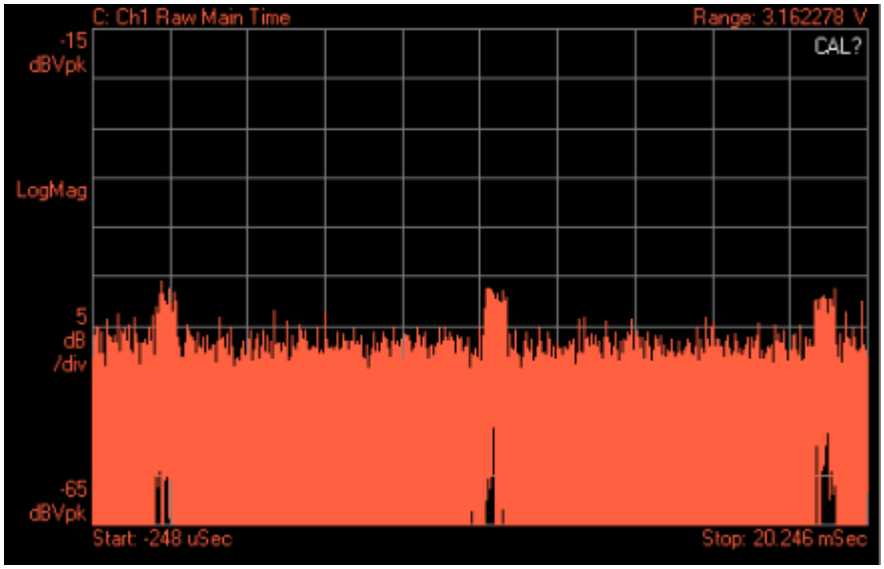


Figura 79: Transmisión del AGCH

En esta imagen se ve que el tiempo de transmisión es bastante mayor que en el canal RACH, ya que, la ráfaga del canal AGCH contiene más bits. La diferencia de amplitud de los pulsos se debe a que la frecuencia de 645 MHz es recibida de peor forma que la de 600 MHz.

Canal SDCCH de subida:

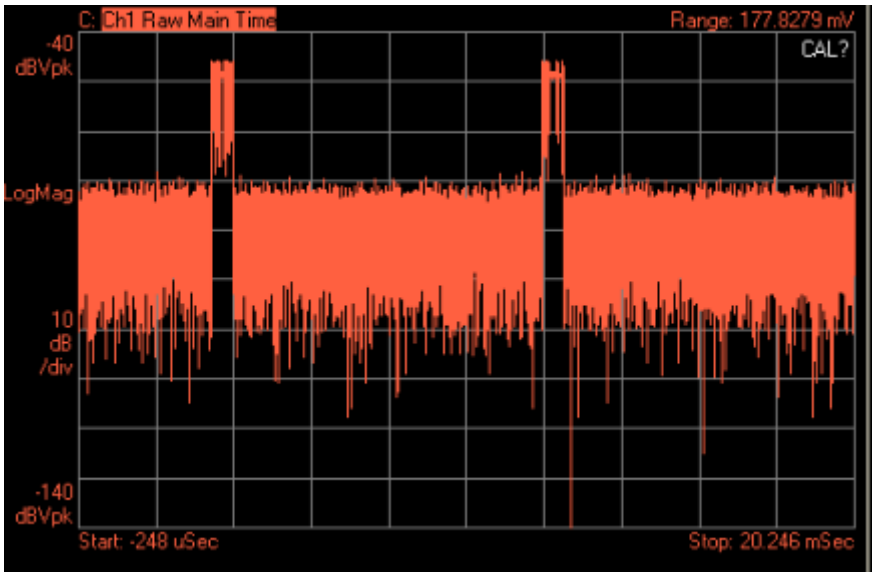


Figura 80: Transmisión del SDCCH (subida)

Canal SDCCH de bajada:

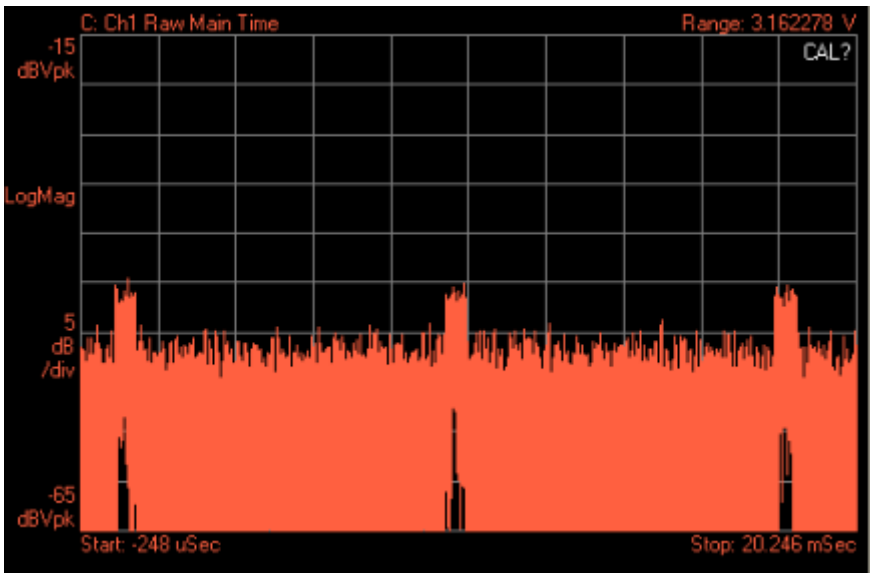


Figura 81: Transmisión del SDCCH (bajada)

Constelación recibida:

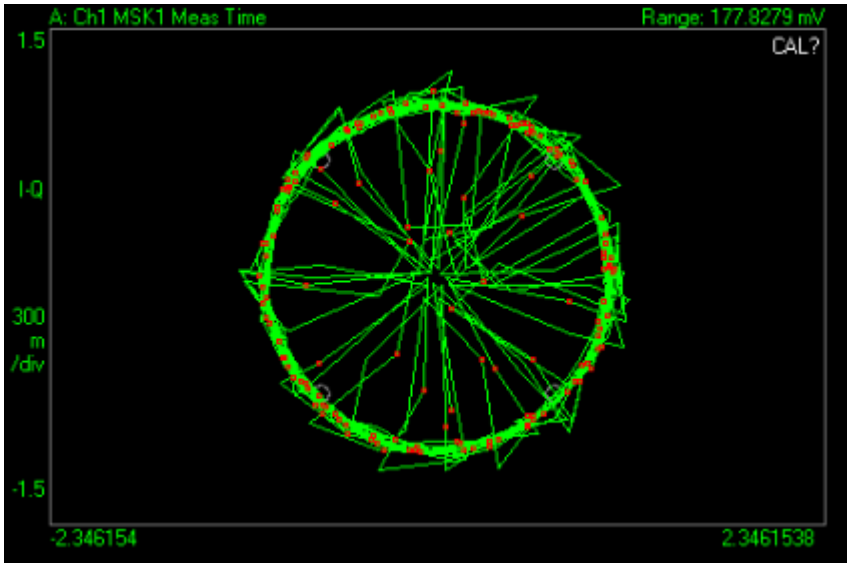


Figura 82: Constelación recibida

La constelación recibida por el analizador vectorial de señales concuerda completamente a la utilizada en la GMSK de GSM.

7 Presupuesto

En este apartado se realiza un presupuesto detallado del TFG. Para ello, se calcularan los costes de personal calculando las horas trabajadas y los tiempos del material utilizado teniendo en cuenta el número de horas utilizado, el periodo de depreciación y el importe de los equipos.

7.1 Costes de personal

Para comenzar se calcula el número de horas dedicado por el graduado a este trabajo desglosándolo por fases.

FASE	TAREA	TIEMPO (Días)
Documentación sobre GSM.	Búsqueda y selección de la documentación de GSM	3
	Estudio a fondo de la documentación	15
Aprendizaje y familiarización de las herramientas de trabajo.	Aprendizaje del lenguaje gráfico de LabVIEW	15
	Familiarización con el hardware utilizado	5
Implementación de los módulos.	Prueba y verificación de los módulos ya realizados	5
	Implementación de los módulos necesarios	60
Pruebas y optimizaciones	-	15
Realización de la memoria	-	30
TOTAL		**148**

Tabla 10: Días dedicados a cada tarea

Teniendo en cuenta que se ha trabajado una media de 3 horas diarias, este trabajo ha supuesto una cantidad de 444 horas.

En este trabajo, además del graduado se ha necesitado la ayuda de un Doctor Ingeniero al que se le imputan, aproximadamente, el 10% de las horas trabajadas por el graduado.

	TIEMPO (horas)	PRECIO/HORA (€)	IMPORTE (€)
Doctor ingeniero	44	120	5280
Graduado	444	60	26640
TOTAL			31920

Tabla 11: Costes de personal

Los costes de personal del proyecto ascienden a un total de 31920 €.

7.2 Costes de material

Para calcular el coste de cada componente utilizado se tienen en cuenta tres variables:

- Tiempo de utilización.
- Periodo de depreciación.
- Importe.

Se calcula según la siguiente fórmula:

$$Coste = \frac{Tiempo\ de\ utilización}{Tiempo\ de\ depreciación} * Importe$$

La siguiente tabla muestra todos los componentes y equipos utilizados, su tiempo de utilización, el periodo de depreciación, su importe inicial y el coste imputable al proyecto.

	Tiempo utilizado (meses)	Periodo de depreciación (meses)	Importe (€)	Coste (€)
Ordenador portátil ASUS	7,5	42	599	106,96
Ordenador portátil ACER	1	42	464	11,05
4 x NI USRP 2920 (incluye antenas, cable MIMO y cable Ethernet)	6	84	12244	874,57
LabVIEW	7	48	3310	482,71
Agilent VSA 89600	2	120	165800	2763,33
TOTAL				4238,62

Tabla 12: Costes de material

Los costes de material del proyecto suponen 4238,62 €.

7.3 Costes totales

Por último, únicamente falta sumar todos los costes para calcular el coste total.

CONCEPTO	COSTE (€)
Coste de personal	31920,00
Cote de materiales	4238,62
Costes indirectos (20%)	7231,72
IVA (21%)	9111,97
TOTAL	52502,31

Tabla 13: Costes totales

Los costes totales de este proyecto ascienden a una cantidad de 52502,31 euros.

8 Conclusiones

8.1 Conclusiones generales

Los resultados mostrados en los capítulos 5 y 6 muestran que, a grandes rasgos, se ha cumplido el objetivo de este trabajo. A pesar de algunas complicaciones, se ha logrado el intercambio de mensajes necesarios entre la estación base y el móvil para realizar el procedimiento de attach descrito.

En cuanto al objetivo de implementar el procedimiento lo más fielmente al estándar posible, no se ha conseguido totalmente.

La creación de los mensajes, su inserción en la ráfaga, su codificación y, finalmente, su modulación se ha conseguido tal y como indica el estándar GSM. Sin embargo, el envío y recepción de los mensajes han dado muchos problemas, por lo que parte de la interfaz radio no se ajusta realmente a GSM. En este caso, la sincronización no ha sido posible, por lo que se ha tenido que diseñar el sistema de forma en que el receptor tiene que detectar patrones para poder conseguir los mensajes que le envía la otra parte.

A pesar de estos problemas, el objetivo de este proyecto, el docente, sí se ha conseguido. El trabajo muestra muchos procesos que se realizan en GSM y se puede usar para acercar a otros alumnos a esta tecnología. Además, este trabajo podrá ser usado en futuros proyectos, tanto para ampliaciones como para introducirlo dentro de otros trabajos.

Tras la realización de este trabajo, el alumno ha conseguido comprobar las ventajas y los inconvenientes de usar tecnologías SDR. Por una parte, se han percibido las grandes posibilidades de estas tecnologías, que, mediante el uso de un ordenador portátil y unos receptores y transmisores se pueden conseguir buenos resultados que se pueden usar en el mundo real. Sin embargo, por otra parte, se ha visto la gran complejidad de software que pueden tener estos sistemas, ya que, aunque pueden abaratar mucho los costes debido al hardware, el software detrás de esto puede llegar a ser muy complejo.

8.2 Futuras líneas de trabajo

Este trabajo puede marcar futuras líneas de trabajo como las siguientes:

- Se puede completar el trabajo realizando la sincronización entre la estación base y el móvil para que el envío y recepción del mensaje se adecúe al estándar GSM.

- Este procedimiento de attach no es único de GSM, por lo que otra posible línea de trabajo sería implementar el procedimiento adecuándolo a otros estándares como GPRS, UMTS o, incluso, LTE.
- Este trabajo únicamente se centra en la interfaz radio. En futuras ampliaciones se podrían incluir otros elementos de la red GSM que participan en este proceso, como el MSC o el HLR.

Como se ve, pueden existir varias líneas de trabajo futuras, aunque pueden limitarse por la capacidad de los transceptores disponibles.

Referencias

[1] Wikipedia, «GSM procedures,» [En línea]. Available: https://en.wikipedia.org/wiki/GSM_procedures. [Último acceso: 15 agosto 2015].

[2] ETSI, «Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification (GSM 04.08),» Julio 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/04/0408/05.03.00_60/gsmts_0408v050300p.pdf. [Último acceso: 20 Agosto 2015].

[3] Departamento de Teoría de la Señal y Comunicaciones. Universidad Carlos III de Madrid, *Comunicaciones Móviles. Tema 2. Sistema GSM: Interfaz Radio (Parte 2),* Madrid, 2015.

[4] GNURadio, «New Filter Design Tool in 'next',» 18 Diciembre 2012. [En línea]. Available: http://gnuradio.squarespace.com/home/2012/12/18/new-filter-design-tool-in-next.html. [Último acceso: 17 Agosto 2015].

[5] SDR-Radio, «SDR-Radio.com,» [En línea]. Available: http://sdr-radio.com/Software. [Último acceso: 17 Agosto 2015].

[6] Jefatura del Estado, «BOE,» 9 Mayo 2014. [En línea]. Available: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-4950. [Último acceso: 17 Agosto 2015].

[7] Ministerio de la Presidencia, «BOE,» 28 Septiembre 2001. [En línea]. Available: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2001-18256. [Último acceso: 17 Agosto 2015].

[8] TechnologyUK, «TechnologyUK,» [En línea]. Available: http://www.technologyuk.net/telecommunications/communication_technologies/gsm.shtml. [Último acceso: 19 Agosto 2015].

[9] T. Farley y v. d. H. Mark, «PrivateLine,» 1 Enero 2016. [En línea]. Available: http://www.privateline.com/mt_cellbasics/2006/01/cell_and_sectorterminology.html. [Último acceso: 19 Agosto 2015].

[10] V. Lado, «GSM, part 1 of 3,» 23 Junio 2009. [En línea]. Available: http://adikristanto.net/gsm-part-1-of-3/. [Último acceso: 20 Agosto 2015].

[11] M. Benjamin, B. Dunbar, B. Palmer y A. Valkov, «Global System for Mobile Communications,» [En línea]. Available: http://services.eng.uts.edu.au/userpages/kumbes/public_html/ra/gsm/gsm.html. [Último acceso: 21 Agosto 2015].

[12] J. M. H. Rábanos, Comunicaciones Móviles, Madrid: Centro de Estudios Ramón Areces, 2004.

[13] ETSI, «Digital cellular telecommunications system (Phase 2+); Modulation (GSM 05.04 version 8.1.2 Release 1999),» Febrero 2001. [En línea]. Available: http://www.etsi.org/deliver/etsi_en/300900_300999/300959/08.01.02_60/en_300959v080102p.pdf. [Último acceso: 15 Mayo 2015].

[14] National Instrument, «NI USRP-292x/293x Datasheet,» [En línea]. Available: http://www.ni.com/datasheet/pdf/en/ds-355. [Último acceso: 27 Agosto 2015].

[15] Agilent, «Agilent 89600S Series VXI-Based,» [En línea]. Available: http://literature.cdn.keysight.com/litweb/pdf/5968-9350E.pdf. [Último acceso: 27 Agosto 2015].

[16] ETSI, «Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification (GSM 03.03),» Marzo 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/03/0303/05.00.00_60/gsmts_0303v050000p.pdf. [Último acceso: 15 Mayo 2015].

[17] ETSI, «Digital cellular telecommunications system; Restoration procedures (GSM 03.07),» Noviembre 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/03/0307/05.00.00_60/gsmts_0307v050000p.pdf. [Último acceso: 15 Mayo 2015].

[18] ETSI, «Digital cellular telecommunications system (Phase 2+); Organization of subscriber data (GSM 03.08),» Abril 1997. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/03/0308/05.01.00_60/gsmts_0308v050100p.pdf. [Último acceso: 15 Mayo 2015].

[19] «Digital cellular telecommunications system; Location registration procedures (GSM 03.12),» Noviembre 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/03/0312/05.00.00_60/gsmts_0312v050000p.pdf. [Último acceso: 15 Mayo 2015].

[20] ETSI, ««Digital cellular telecommunications system (Phase 2+); Security related network functions (GSM 03.20),» Julio 2001. [En línea]. Available: http://www.etsi.org/deliver/etsi_ts/100900_100999/100929/08.01.00_60/ts_100929v080100p.pdf. [Último acceso: 15 Mayo 2015].

[21] ETSI, «Digital cellular telecommunications system; Functions related to Mobile Station (MS) in idle mode and group receive mode (GSM 03.22),» Mayo 1997. [En línea]. Available: http://www.etsi.org/deliver/etsi_i_ets/300900_300999/300930/01_60/ets_300930e01p.pdf. [Último acceso: 15 Mayo 2015].

[22] ETSI, «Digital cellular telecommunications system (Phase 2+); Physical layer on the radio path; General description (GSM 05.01),» Abril 1998. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/05/0501/05.04.00_60/gsmts_0501v050400p.pdf. [Último acceso: 15 Mayo 2015].

[23] ETSI, «Digital cellular telecommunications system (Phase 2+); Multiplexing and multiple access on the radio path (GSM 05.02),» Agosto 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/05/0502/05.01.00_60/gsmts_0502v050100p.pdf. [Último acceso: 15 Mayo 2015].

[24] ETSI, ««Digital cellular telecommunications system (Phase 2+); Channel coding (GSM 05.03),» Agosto 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/05/0503/05.02.00_60/gsmts_0503v050200p.pdf. [Último acceso: 15 Mayo 2015].

[25] ETSI, ««Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification (GSM 09.02),» Agosto 1996. [En línea]. Available: http://www.etsi.org/deliver/etsi_gts/09/0902/05.03.00_60/gsmts_0902v050300p.pdf. [Último acceso: 15 Mayo 2015].

[26] W. C. Lee, «GlobalSpec,» [En línea]. Available: http://www.globalspec.com/reference/81097/203279/4-2-global-system-for-mobile-gsm. [Último acceso: 20 Agosto 2015].

[27] Tutorials Point, «GSM - The Mobile Station,» [En línea]. Available: http://www.tutorialspoint.com/gsm/gsm_mobile_station.htm. [Último acceso: 20 Agosto 2015].

[28] National Instruments, «USRP-2920,» [En línea]. Available: http://sine.ni.com/nips/cds/view/p/lang/es/nid/209948. [Último acceso: 27 Agosto 2015].